

# Velociraptor

Digging Deeper!



# Velociraptor Installation and overview

Introducing the little green reptile!



# Module overview

In this module we introduce the tool and explain the rationale behind its design.

We will deploy Velociraptor in a cloud environment - We aim to be as close to how one would deploy it on a real deployment as possible.

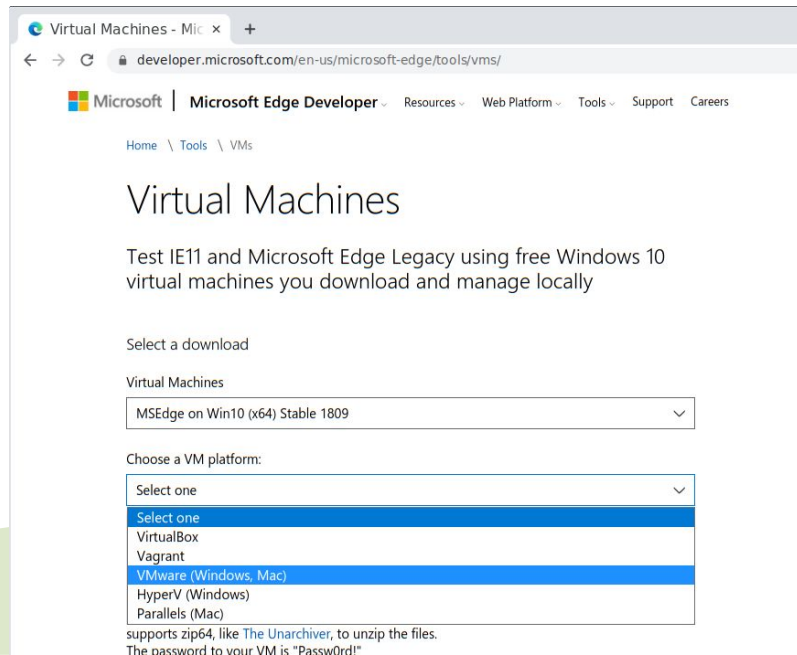
We will play with the GUI and introduce some of the main concepts



# Prerequisites

In order to follow along with this workshop you will need to use a windows VM with administrator level access.

You can grab a free VM from [Microsoft](https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/)





# Prerequisites

In the first part of this session I will be installing Velociraptor in the cloud environment on GCP.

Because of the size of this course we can not provide people with the cloud infrastructure so you will need to do this on your own cloud account later - this is a demonstration only.

There are a lot of screenshots in the slides to allow you to replicate this later with your setup - we recommend practicing this a couple of times.



# What is Velociraptor?

**Velociraptor is a unique DFIR tool, giving you power and flexibility through the Velociraptor Query Language (VQL)**

VQL is used for everything:

- ❑ Collecting information from endpoints (also called *clients*)
- ❑ Controlling monitoring and response on endpoints
- ❑ Controlling and managing the Velociraptor server.



# History

Velociraptor draws inspiration from two major projects:

- ❑ GRR <https://github.com/google/grr>
- ❑ OSQuery <https://github.com/osquery/osquery>



# Velociraptor vs GRR

## In common

- ❑ Hunting across large number of endpoints
- ❑ Can collect file data
- ❑ Free Open source (FOSS)

## Different

- ❑ Much faster
- ❑ Lower footprint
- ❑ A flexible query language
- ❑ Very simple to deploy
- ❑ Event based queries
- ❑ Commercially supported FOSS



# Velociraptor vs OSQuery

## In common

- ❑ Rely on a query language to access machine state
- ❑ Single binary with no dependencies
- ❑ Multi-platform

## Different

- ❑ VQL is much more powerful and intuitive than SQL
- ❑ Much faster than OSQuery
- ❑ Can transfer file data
- ❑ Can modify the system
- ❑ Remote client/server control and orchestration in the same tool.



# Velociraptor vs OSQuery



Powerful



Control



Same



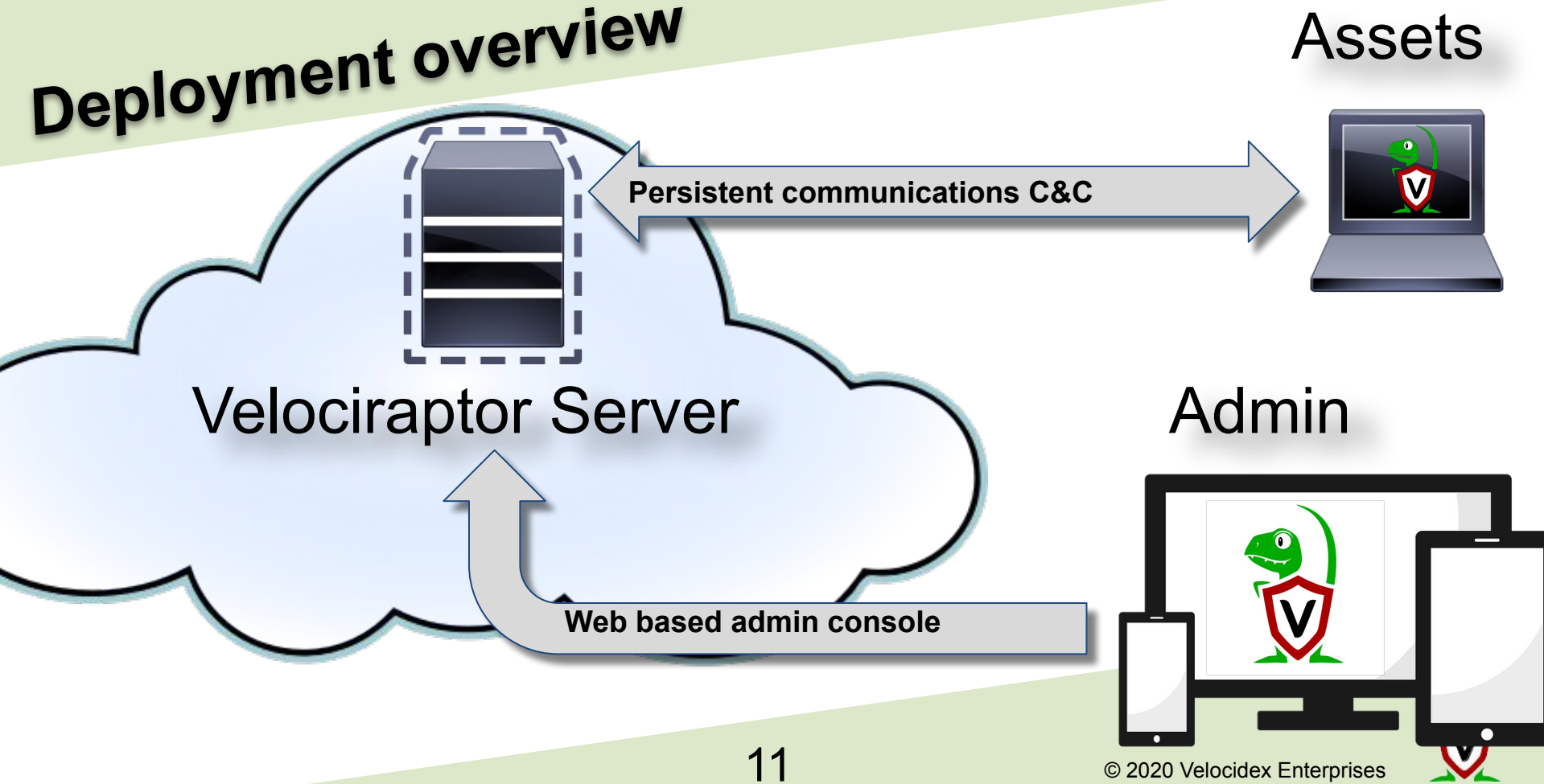
Powerful

Control  
Same

risers



# Deployment overview



# Typical deployments

Velociraptor is very efficient and scalable:

- ❑ Server simply collects the results of queries - clients do all the heavy lifting.
  - ❑ Client memory and CPU usage is controlled via throttling and active cancellations.
- ❑ Server is optimized for speed and scalability
  - ❑ Concurrency control ensures stability
  - ❑ Bandwidth limits ensure network stability





# Typical deployments

## Current recommendations

- ❑ 10k-15k clients - single server with file based data store (usually cloud VM).
  - ❑ SSL load is the biggest load - TLS offloading helps a lot!
  - ❑ 8 GB RAM/8 cores is generous towards the top of the range.
- ❑ We recommend Ubuntu/Debian server



# Multi-Frontend configuration

- ❑ Available since 0.5.9 - suitable for > 10k endpoints
- ❑ Still considered experimental - help us test it!
- ❑ Master/Minion model
- ❑ Outside the scope of this course but you can find more information in our [blog post](#)



# Deploying Velociraptor



# Run Velociraptor on your machine

Download Velociraptor from GitHub (.msi or .exe)

**"C:\program files\Velociraptor\Velociraptor.exe" gui**



```
C:\Program Files\Velociraptor>Velociraptor.exe gui
```

```
INFO] 2020-09-08T05:36:06-07:00
INFO] 2020-09-08T05:36:06-07:00
INFO] 2020-09-08T05:36:06-07:00
INFO] 2020-09-08T05:36:06-07:00
INFO] 2020-09-08T05:36:06-07:00
INFO] 2020-09-08T05:36:06-07:00
INFO] 2020-09-08T05:36:06-07:00 Digging deeper! https://www.velocidex.com
INFO] 2020-09-08T05:36:06-07:00 This is Velociraptor 0.4.9 built on 2020-09-02T14:19:59+10:00 (6a559265)
INFO] 2020-09-08T05:36:06-07:00 No embedded config - you can pack one with the `config repack` command
INFO] 2020-09-08T05:36:06-07:00 Env var VELOCIRAPTOR_CONFIG is not set
INFO] 2020-09-08T05:36:06-07:00 Loading config from file C:\Users\test\AppData\Local\Temp\server.config.yaml
INFO] 2020-09-08T05:36:06-07:00 No valid config found - will generate a new one at C:\Users\test\AppData\Local\Temp\server.config.yaml
INFO] 2020-09-08T05:36:06-07:00 Starting Frontend. {"build_time":"2020-09-02T14:19:59+10:00","commit":"6a559265","version":"0.4.9"}
INFO] 2020-09-08T05:36:06-07:00 Starting Journal service.
INFO] 2020-09-08T05:36:06-07:00 Starting the notification service.
INFO] 2020-09-08T05:36:06-07:00 Starting Inventory Service
INFO] 2020-09-08T05:36:06-07:00 Loaded 185 built in artifacts in 97.1217ms
INFO] 2020-09-08T05:36:06-07:00 Starting Label service.
INFO] 2020-09-08T05:36:06-07:00 Starting Hunt Dispatcher Service.
INFO] 2020-09-08T05:36:06-07:00 Selected frontend configuration localhost:8000
INFO] 2020-09-08T05:36:06-07:00 Starting Client Monitoring Service
INFO] 2020-09-08T05:36:06-07:00 Creating default Client Monitoring Service
INFO] 2020-09-08T05:36:06-07:00 Initial user admin not present, creating
INFO] 2020-09-08T05:36:06-07:00 Server upgrade detected -> 0.4.9... running upgrades.
INFO] 2020-09-08T05:36:06-07:00 Upgrading tool OSQueryLinux {"Tool":{"name":"OSQueryLinux","github_project":"Velocidex/OSQuery-Releases","github_asset_regex":"linux-amd64"}}
```



# Self Signed SSL mode

- ❑ Frontend served using TLS on port 8000 (connected to clients)
- ❑ GUI uses basic authentication with usernames/passwords.
- ❑ GUI Served over loopback port 8889 (127.0.0.1)
  - ❑ By default not exposed to the network
  - ❑ You can use SSH tunneling to forward the GUI



# Steps to deploy Velociraptor

1. Provision a VM in the cloud
  - a. Configure DNS (static or dynamic)
  - b. Configure OAuth2 SSO
2. Generate configuration files
3. Build debian packages and install
4. Build MSI packages for Windows
5. Deploy via GPO/SCCM etc.

The instructor will demonstrate step 1. See the workshop setup document for credentials.



# Setting Dynamic DNS with Google Domains

← → ↺ 🔒 domains.google.com/registrar/velocidex-training.com/dns?authuser=1 🔍 ☆ 📄 🗨️ 25 📧 🏠 ⚙️ 👤

☰ Google Domains ⋮ 🌐

← All my domains

velocidex-training.com

🗂️ Domain overview

⚙️ Registration settings

📖 DNS

🌐 Website

📊 Reports

✉️ Email

🛡️ Security

🔍 Get a new domain

💬 Send feedback

Synthetic records

Synthetic records allow you to add common features, such as domain forwarding or G Suite, to your domain in one step. Each synthetic record is an automatically-generated collection of resource records related to a specific feature. [Learn more](#)

Dynamic DNS ▼ vm2 .velocidex-training.com

Add

> Domain forward

velocidex-training.com, www.velocidex-training.com → https://www.velocidex.com/training/ [View setting](#) [Delete](#)

▼ Dynamic DNS

vm1.velocidex-training.com [Delete](#) [Edit](#)

Need help setting this up?

Username: ..... Password: ..... [View credentials](#)

Name ?	Type ?	TTL ?	Data ?
vm1	A	1m	0.0.0.0

© 2020 Velocidex Enterprises



Google Cloud Platform training

# APIs & Services

## OAuth consent screen

**Your consent screen is being verified. This may take up to several weeks. Your last approved consent screen is still in use.**

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

**Application type**

☒ **Public**  
Any Google Account can grant access to the scopes required by this app.  
[Learn more about scopes](#)

☐ **Internal**  
Only users with a Google Account in your organization can grant access to the scopes requested by this app.

**Verification status**  
Being verified (Last approved consent screen is still in use)

**Application name** ⓘ  
The name of the app asking for consent

**Application logo** ⓘ  
An image on the consent screen that will help users recognize your app

**Support email** ⓘ  
Shown on the consent screen for user support

**Scopes for Google APIs**  
Scopes allow your application to access your user's private data. [Learn more](#)  
If you add a sensitive scope, such as scopes that give you full access to Calendar or Drive,

**About the consent screen**  
The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.

**OAuth verification**  
To protect you and your users, your consent screen and application may need to be verified by Google. Verification is required if your app is marked as **Public** and at least one of the following is true:

- Your app uses a sensitive and/or restricted scope
- Your app displays an icon on its OAuth consent screen
- Your app has a large number of authorized domains
- You have made changes to a previously-verified OAuth consent screen

The verification process may take up to several weeks, and you will receive email updates as it progresses. [Learn more](#) about verification.

Before your consent screen and application are verified by Google, you can still test your application with limitations. [Learn more](#) about how your app will behave before it's verified.

[Let us know what you think](#) about our OAuth experience.

**OAuth grant limits**  
**Token grant rate**  
Your current per minute token grant rate limit is 100 grants per minute. The per minute token grant rate resets every minute. Your current per day token grant

# Configuring Google OAuth2 requires a new project and a consent screen

Do not add an application logo or require more permissions - Google will require OAuth verification which can take weeks!



Google Cloud Platform training

APIs & Services

Dashboard

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Credentials

+ CREATE CREDENTIALS

DELETE

Create credentials to access Google APIs

API Keys

☐ Name

No API keys displayed

OAuth 2.0 Client IDs

☐ Name

Creation date ↓

Type

Client ID

Usage with all services (last 30 days) ?

vm1.training.velocidex.com

Jan 31, 2020

Web application

1072201830115-q74...

0

Service Accounts

☐ Email

Name ↑

Usage with all services (last 30 days) ?

1072201830115-compute@developer.gserviceaccount.com

Compute Engine default service account

0

API key

Identifies your project using a simple API key to check quota and access

OAuth client ID

Requests user consent so your app can access the user's data

Service account

Enables server-to-server, app-level authentication using robot accounts

Help me choose

Asks a few questions to help you decide which type of credential to use

Generate OAuth client credentials.  
Note you can have multiple credentials and multiple domains in the same GCP project.



## Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See [Setting up OAuth 2.0](#) for more information.

## Application type

- ☒ Web application
- ☐ Android [Learn more](#)
- ☐ Chrome App [Learn more](#)
- ☐ iOS [Learn more](#)
- ☐ Other

## Name

## Restrictions

Enter JavaScript origins, redirect URIs, or both [Learn More](#)

Origins and redirect domains must be added to the list of Authorized Domains in the [OAuth consent settings](#).

## Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard ([https://\\*.example.com](https://*.example.com)) or a path (<https://example.com/subdir>). If you're using a nonstandard port, you must include it in the origin URI.

Type in the domain and press Enter to add it

## Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

Type in the domain and press Enter to add it

Create

Cancel

The redirect URL is the url which Google will use to call back to Velociraptor with the user's successful login.

It must be

`https://<domain>/auth/google/callback`



Create credentials to access your enabled APIs. [Learn more](#)

## API Keys

☐

No API keys

## OAuth

☐☐☐☐

## Service accounts

☐☐

### OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services



OAuth is limited to 100 [sensitive scope logins](#) until the [OAuth consent screen](#) is published. This may require a verification process that can take several days.

Your Client ID

1072201830115-p7a13he2jhr41uik7dcf3cqf64k4n5bq.apps.g



Your Client Secret

P91U8LW207H0qq6gK42gHTke



OK

Note the client id and secret - we will need to provide it in the server config.



# Installing a new server

Use the password provided in the Workshop setup to log into the server.

1. Fetch the latest Velociraptor Windows and Linux release binaries
2. Create a new configuration
  - a. `velociraptor config generate -i`
3. Create a new server debian package
  - a. `velociraptor --config server.config.yaml debian server`



# Installing a new server

1. Push the debian package to the server using scp
  - a. `scp velociraptor_server*.deb mike@123.45.67.89:/tmp/`
2. Install package
  - a. `sudo dpkg -i velociraptor_server*.deb`



Latest release

v0.5.5-1

98119e5

Verified

Compare ▼

# Release 0.5.5-1


 scudette released this 9 days ago · [9 commits](#) to master since this release


This is a bugfix release from 0.5.5. Thanks for the bug reports and feedback.


Major issues fixed:

1. Memory leak in foreach() plugin
2. Python gRPC API handler crash
3. GUI Fix welcome screen logo was shown with incorrect size
4. GUI Fix VFS browser showing paths with % in their name
5. File based merge sort would fix memory issue on large ORDER BY queries.


## Assets 7


 [velociraptor-v0.5.5-1-darwin-amd64](#)


 [velociraptor-v0.5.5-1-linux-amd64](#)

 [velociraptor-v0.5.5-1-windows-386.exe](#)

 [velociraptor-v0.5.5-1-windows-amd64.exe](#)

 [velociraptor-v0.5.5-1-windows-amd64.msi](#)

 [Source code](#) (zip)

 [Source code](#) (tar.gz)





```

C:\Users\mike\Downloads>velociraptor-v0.4.3.3-windows-amd64.exe config generate -i
? Please select the datastore implementation
  FileBaseDataStore
? Path to the datastore directory. /data/
?
Welcome to the Velociraptor configuration generator
-----

I will be creating a new deployment configuration for you. I will
begin by identifying what type of deployment you need.

Authenticate users with Google OAuth SSO
? What is the public DNS name of the Frontend (e.g. www.example.com): [? for help] (www.example.com) vm1.training.veloci
? What is the public DNS name of the Frontend (e.g. www.example.com): vm1.training.velocidex.com
? Enter the Google OAuth Client ID? 1072201830115-q74o1slmu2u3...s.googleusercontent.com
? Enter the Google OAuth Client Secret? 4VHuIw...SWTUG
? Are you using Google Domains DynDNS? Yes
? Google Domains DynDNS Username iYayz1Lj...tT
? Google Domains DynDNS Password 2Xst1...
? GUI Username or email address to authorize (empty to end):
? Path to the logs directory. /data/logs
? Where should i write the server config file? server.config.yaml
? Where should i write the client config file? client.config.yaml

```

Generate new configuration with the details in the Workshop setup document.

Make sure to use /data/ as this will run on Linux





# Automating config generation

- ❑ Some people want to automate the config generation step.
- ❑ Velociraptor supports a JSON merge for non interactive configuration generation

```
velociraptor config generate --merge  
'{"autocert_domain": "domain.com", "autocert_cert_cache": "/foo/bar"}'
```



# Building a server deb package

```
./velociraptor-v0.5.5-windows.exe --config  
~/server.config.yaml debian server  
--binary velociraptor-v0.5.5-windows.exe
```

```
C:\Users\mike\Downloads>velociraptor-v0.4.3.3-windows-amd64.exe --config server.config.yaml debian server  
--binary velociraptor-v0.4.3-linux-amd64.3
```

```
C:\Users\mike\Downloads>dir *.deb
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 083C-9DFA
```

```
Directory of C:\Users\mike\Downloads
```

```
05/28/2020  01:36 AM          15,034,866 velociraptor_0.4.3_server.deb
```

```
1 File(s)          15,034,866 bytes
```

```
0 Dir(s)  35,973,652,480 bytes free
```

```
C:\Users\mike\Downloads>_
```

# Deploying the server

scp the deb file to the target server

```
C:\Users\mike\Downloads>scp velociraptor_0.4.3_server.deb mike@34.71.243.48:
The authenticity of host '34.71.243.48 (34.71.243.48)' can't be established.
ECDSA key fingerprint is SHA256:OaQExNPmx95YD9qZF16YGZT7ML5dFbj1XwMtGPsuY9Q.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '34.71.243.48' (ECDSA) to the list of known hosts.
mike@34.71.243.48's password:
velociraptor_0.4.3_server.deb                                100% 14MB 70.6MB/s 00:00
```



```
Last login: Thu May 28 21:11:22 EDT 11 00 / 71.162.71.22
mike@vm1-training:~$ sudo dpkg -i ./velociraptor_0.4.3_server.deb
Selecting previously unselected package velociraptor-server.
(Reading database ... 37691 files and directories currently installed.)
Preparing to unpack .../velociraptor_0.4.3_server.deb ...
Unpacking velociraptor-server (0.4.3) ...
dpkg: dependency problems prevent configuration of velociraptor-server:
 velociraptor-server depends on libcap2-bin; however:
  Package libcap2-bin is not installed.

dpkg: error processing package velociraptor-server (--install):
 dependency problems - leaving unconfigured
Errors were encountered while processing:
 velociraptor-server
mike@vm1-training:~$ sudo apt-get install -f
Reading package lists... Done
Building dependency tree
Reading state information... Done
Correcting dependencies... Done
The following additional packages will be installed:
 libcap2-bin libpam-cap
The following NEW packages will be installed:
 libcap2-bin libpam-cap
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
1 not fully installed or removed.
Need to get 40.0 kB of archives.
After this operation, 128 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

When installing the deb package you might need to install dependencies by using "apt-get install -f"



```
Setting up libcap2-bin (1:2.25-1) ...
Setting up velociraptor-server (0.4.3) ...
Adding group `velociraptor' (GID 112) ...
Done.
Adding system user `velociraptor' (UID 108) ...
Adding new user `velociraptor' (UID 108) with group `velociraptor' ...
Not creating home directory `/etc/velociraptor/'.
Created symlink /etc/systemd/system/multi-user.target.wants/velociraptor_server.service → /etc/systemd/system/velociraptor_server.service.
Processing triggers for man-db (2.7.6.1-2) ...
mike@vm1-training:~$ sudo service velociraptor server status
• velociraptor_server.service - Velociraptor linux amd64
  Loaded: loaded (/etc/systemd/system/velociraptor_server.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2020-05-28 01:43:35 UTC; 36s ago
  Main PID: 1556 (velociraptor)
  Tasks: 9 (limit: 4915)
  CGroup: /system.slice/velociraptor_server.service
          └─1556 /bin/bash /usr/local/bin/velociraptor --config /etc/velociraptor/server.config.yaml frontend
          └─1557 /usr/local/bin/velociraptor.bin --config /etc/velociraptor/server.config.yaml frontend

May 28 01:43:35 vm1-training systemd[1]: Started Velociraptor linux amd64.
mike@vm1-training:~$
```

The service adds a new velociraptor user to run under.  
You can now access the Velociraptor server using your browser.



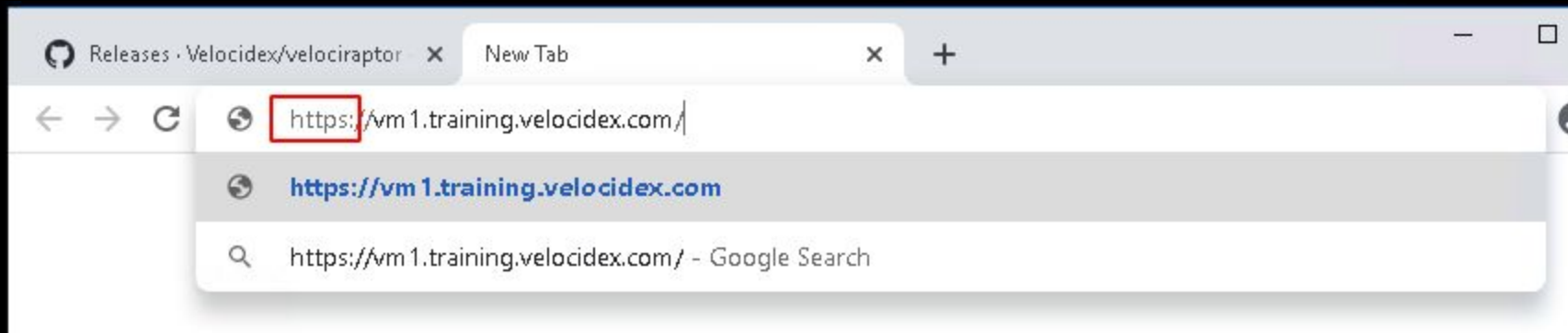
```
mic@velotest:~$ ./velociraptor-v0.4.3-linux-amd64 --config server.config.yaml debian server
mic@velotest:~$ sudo dpkg -i velociraptor_0.4.2_server.deb
Reading database ... 39245 files and directories currently installed.)
Preparing to unpack velociraptor_0.4.2_server.deb ...
Removed /etc/systemd/system/multi-user.target.wants/velociraptor_server.service.
Unpacking velociraptor-server (0.4.2) over (0.4.1) ...
Setting up velociraptor-server (0.4.2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/velociraptor_server.service → /etc/systemd/system/velociraptor_server.service

mic@velotest:~$ sudo service velociraptor_server status
● velociraptor_server.service - Velociraptor linux amd64
   Loaded: loaded (/etc/systemd/system/velociraptor_server.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-05-11 13:36:33 UTC; 15s ago
 Main PID: 5492 (velociraptor)
    Tasks: 9 (limit: 4915)
   CGroup: /system.slice/velociraptor_server.service
           └─5492 /bin/bash /usr/local/bin/velociraptor --config /etc/velociraptor/server.config.yaml frontend
             └─5493 /usr/local/bin/velociraptor.bin --config /etc/velociraptor/server.config.yaml frontend

May 11 13:36:33 velotest systemd[1]: Started Velociraptor linux amd64.
```

Build a Debian package using the new configuration file.  
Install the package  
Check the new service is running properly.

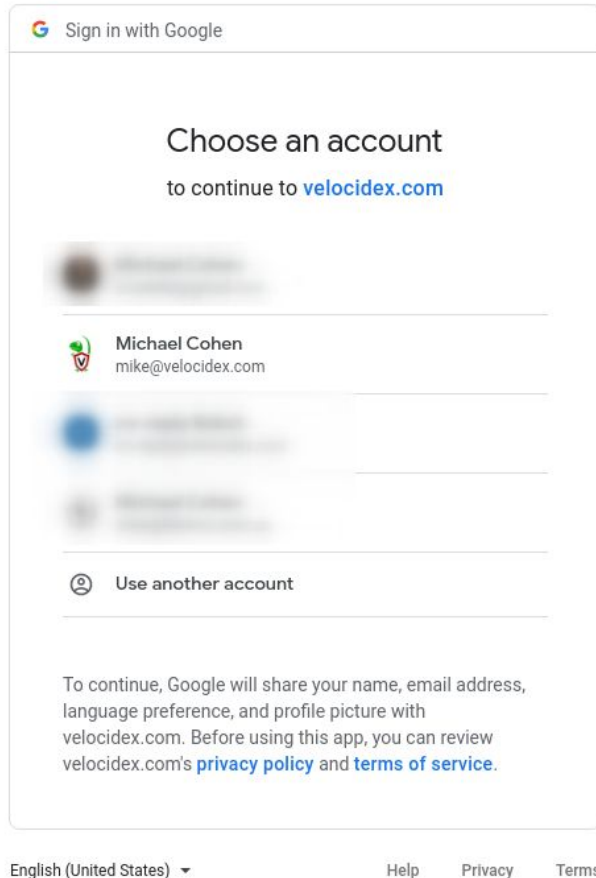




The first time you navigate to the SSL URL the server will obtain a certificate from Let's Encrypt. There will be a small pause as this happens.







You will be redirected to Google for authentication - Velociraptor does not handle any credentials in this configuration. Google will determine if the user authenticated properly (2 FA etc) and convey simple info like the user's email address and avatar.





# User permissions

When running the deb package Velociraptor is running as a non-root user with limited permissions. You must change to this user before manipulating any data, or the service may not be able to open the modified files.

- ❑ Velociraptor will refuse running as another user or as root to prevent permission problems

**sudo -u velociraptor ...**

```
mic@velotest:~$ velociraptor user add joe@example.com --role reader
'/etc/velociraptor/server.config.yaml' is not readable, you will need to run this as the velociraptor user ('sudo -u velociraptor bash').
mic@velotest:~$ sudo velociraptor user add joe@example.com --role reader
velociraptor.bin: error: Velociraptor should be running as the 'velociraptor' user but you are 'root'. Please change user with sudo first
mic@velotest:~$ sudo -u velociraptor velociraptor user add joe@example.com --role reader
Authentication will occur via Google - therefore no password needs to be set.
mic@velotest:~$
```

# Role based Access Control

Velociraptor uses a simple role based access control scheme for now

- ❑ Various Actions require specific permissions
- ❑ Users are granted roles which bestow them with a set of permissions.



# Granting a user role

1. Currently roles are hard coded
  - a. **administrator** - Can do anything without limits
  - b. **reader** - Can read collected data and notebooks
  - c. **api** - Can connect over the API (more later)
  - d. **analyst** - reader + create bulk downloads, edit notebooks
  - e. **investigator** - analyst + schedule new collections and hunts
  - f. **artifact\_writer** - powerful role that allows the user to create and modify artifacts (more on this later)



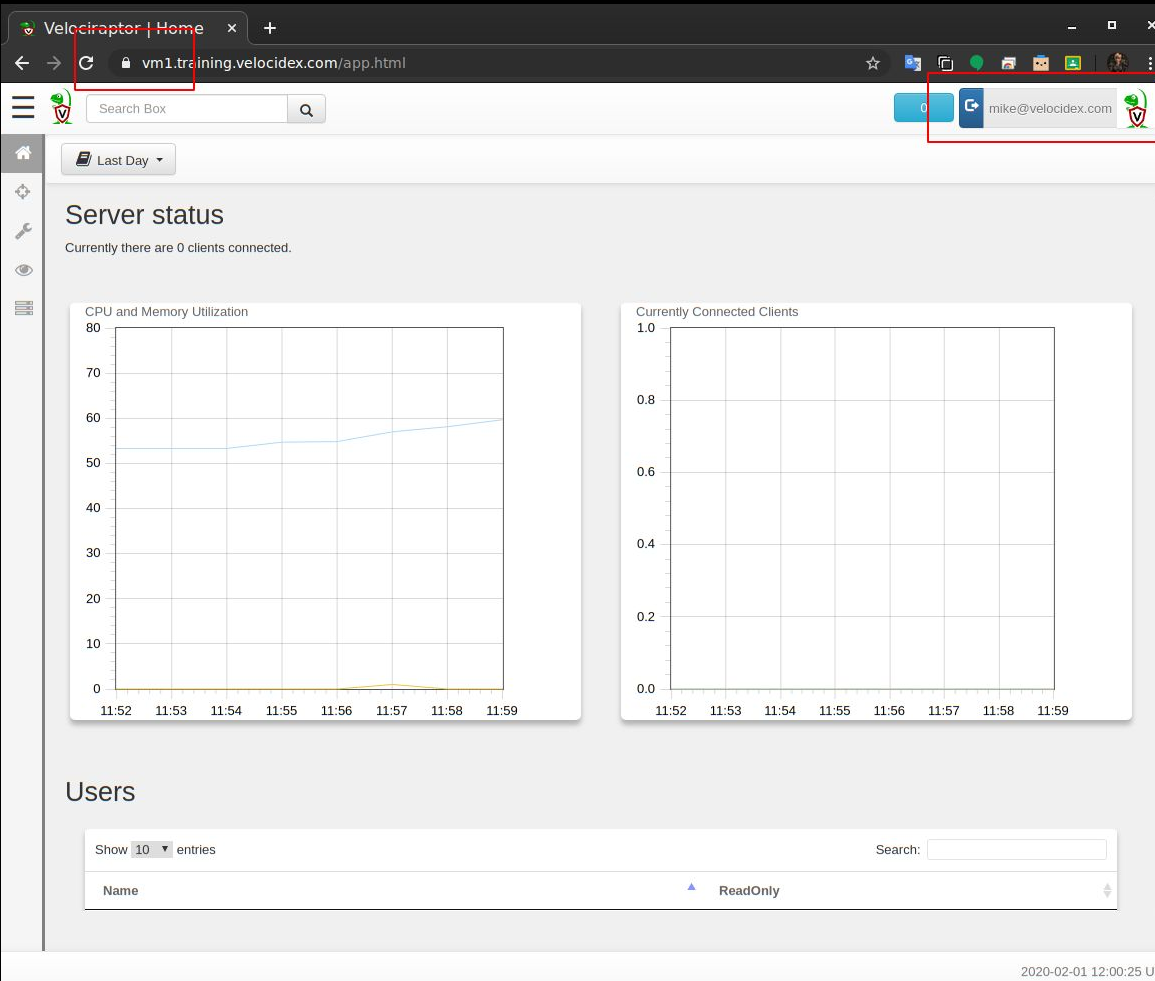
Just because a user is authenticated by Google does not mean they have access to the Velociraptor console!

You must authorize each user to access the console by granting them at least the **reader** role.

Manipulate acls using the "acl show" "acl grant" command

```
elociraptor@velotest:/home/mic$ velociraptor acl grant mike@velocidex.com --role reader,investigator
elociraptor@velotest:/home/mic$ velociraptor acl show mike@velocidex.com
"roles":["reader","investigator"]
elociraptor@velotest:/home/mic$ velociraptor acl show --effective mike@velocidex.com
"any_query":true,"read_results":true,"label_clients":true,"collect_client":true,"notebook_editor":true,"prepare_results":true}
elociraptor@velotest:/home/mic$
```





**Your Velociraptor server is ready.**

You should have a valid SSL Cert and Avatar provided by Google OAuth2



# Velociraptor internals

Digging into Velociraptor!



# The file store

Velociraptor uses a filestore abstraction to store data. By default, we use a simple directory structure in the filesystem.

- ❑ Having simple files simplifies data retention, data migration, backups etc.
- ❑ Makes it easy to integrate with another system (use scp or rsync to just copy files around).
- ❑ If files are deleted, Velociraptor will just recreate them - it is safe to just remove everything!







Now let's configure some clients.





# Deploying clients

We typically distribute signed MSI packages which include the client's config file inside them.

This makes it easier to deploy as there is only one package to install.

We also change name of service/binary etc to make the service a little bit harder to stop.



# Deploying clients

It is possible to embed the config in the clients using the **velociraptor config repack** command (more later)

## Pros

- ❑ Only a single binary no need for an additional config file

## Cons

- ❑ You have to sign the binary again since the config alters the binary.



# Resigning binaries

After buying a code signing cert you can use a script to sign automatically.

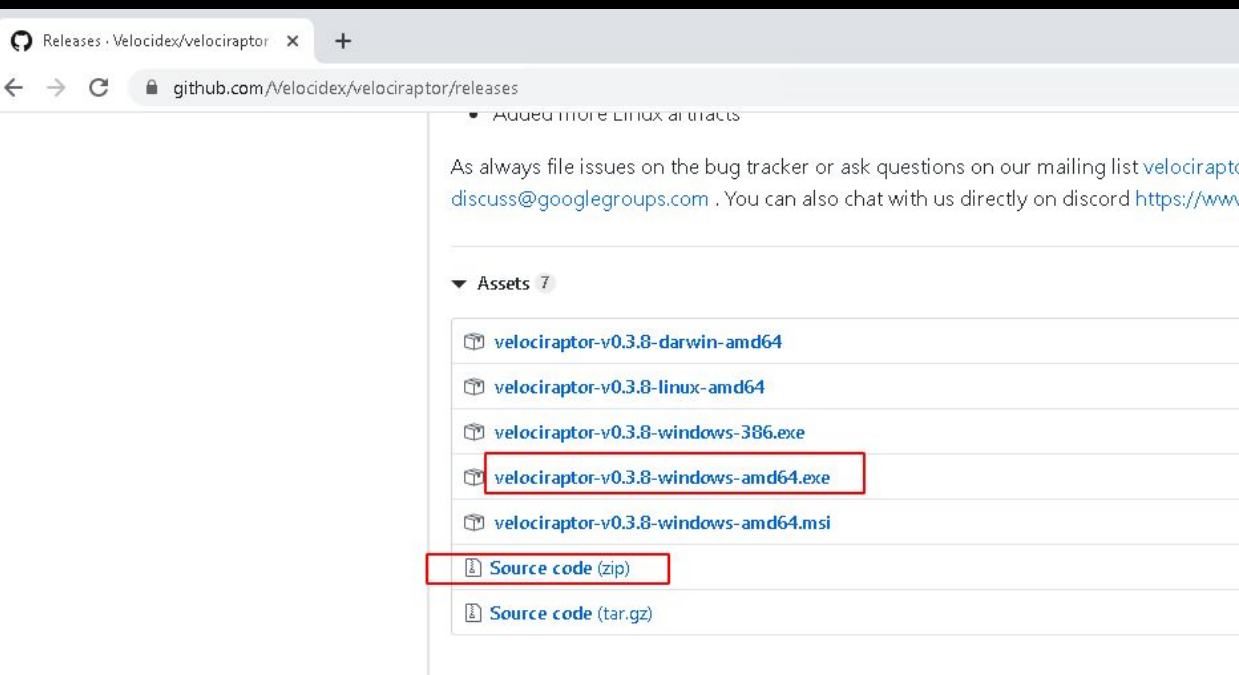
We recommend having a standalone isolated signing machine or VM with FDE

```
#!/bin/bash

osslsigncode sign -pkcs12 ~/private/code_sign.pkcs12 -n "Velociraptor" \
  -h sha2 -t http://timestamp.verisign.com/scripts/timestamp.dll \
  -i https://www.velocidex.com/ \
  -in "$1" -out "$1.signed.exe" -askpass

mv "$1.signed.exe" "$1"
```





**On your windows machine,  
Download the latest binary and the source code.**

[github.com/velocidex/velociraptor/releases](https://github.com/velocidex/velociraptor/releases)



# Velociraptor's public directory

It is handy to have somewhere to serve files from. Velociraptor has a public directory where files are served **without any authentication requirements**

- ❑ We can use this to distribute third party binaries
- ❑ We can serve velociraptor MSI files
- ❑ We can serve various support files (yara rules etc).



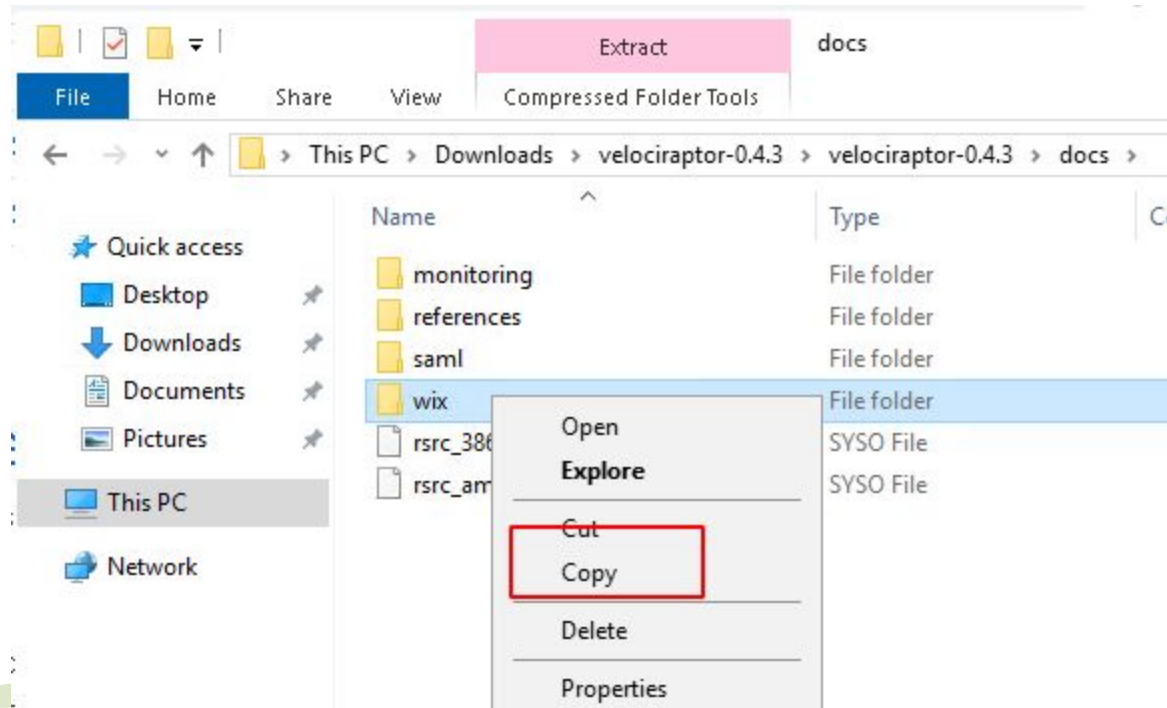
# Velociraptor's public directory

Select the Admin.Client.Upgrade artifact and upload the MSI to the tools setup page (We will learn about that in the next few sessions).

This will now produce a random URL you can serve the MSI from.



# Copy WIX source to desktop.

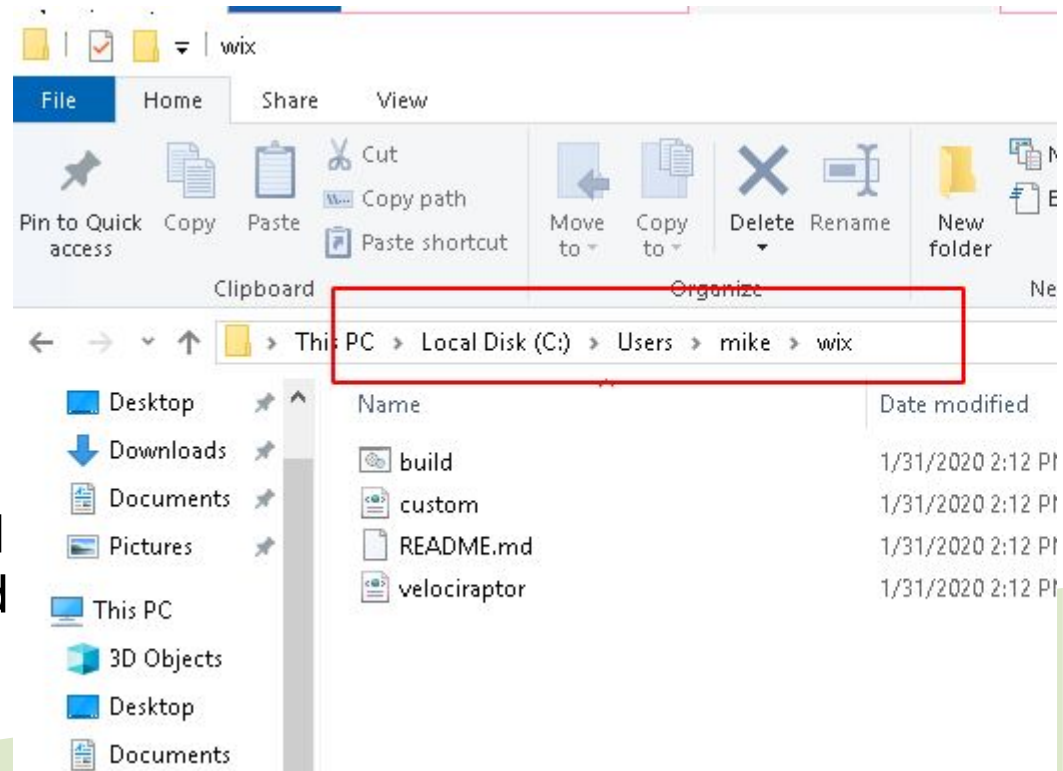


# Build an MSI using Wix Toolkit

Extract the docs/wix directory from the Velociraptor source tree.

These are the required files to construct a new MSI

The main file we use is custom.xml . This file will embed the config file within the MSI and deploy it to the correct directory.





File Release\velociraptor.xml - Notepad++

Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

velociraptor.xml

```
<?xml version='1.0' encoding='windows-1252'?>
<?define AppRegKey="Software\Velocidex\Velociraptor" ?>
<?define PackageDescription="Velociraptor Service Installer" ?>
<?define Manufacturer="Velocidex" ?>
<?define Name="Velociraptor" ?>
<?define Version="0.50.1" ?>
<?define BinaryName="Velociraptor.exe" ?>

<Wix xmlns="http://schemas.microsoft.com/wix/2006/wi"
xmlns:util="http://schemas.microsoft.com/wix/UtilExtension"
>
  <Product Name='$ (var.Name)' Manufacturer='$ (var.Manufacturer)'
    Id='*'
    UpgradeCode='82E586E1-1700-4041-9042-8946BE19B69F'
    Language='1033' Codepage='1252' Version='$ (var.Version)'>
    <Package Id='*' Keywords='Installer' Description="$ (var.PackageDescription)"
      Comments='$ (var.PackageDescription)'
      Manufacturer='$ (var.Manufacturer)'
      InstallerVersion='200' Languages='1033' Compressed='yes'
      SummaryCodepage='1252' />
    <Media Id='1' Cabinet='Sample.cab' EmbedCab='yes' DiskPrompt='CD-ROM #1' />
    <Property Id='DiskPrompt' Value="Installation [1]" />

    <Directory Id='TARGETDIR' Name='SourceDir'>
      <Directory Id='ProgramFiles64Folder' Name='PFiles'>
        <Directory Id='INSTALLDIR' Name='$ (var.Name)'>
          <Directory Id="CACHEDIR" Name="Tools">
            <Component Id="Tools" Guid="97dc953a-8a2f-494f-9585-56ae526d0b48">
              <CreateFolder />
            </Component>
          </Directory>
          <Component Id='MainExecutable'
            Guid='12509926-d242-4f6d-9b5b-6ad2724599a1'
            SourceFile='$(var.BinaryName)' />
        </Directory>
      </Directory>
    </Product>
  </Wix>
```

There are many knobs to tweak here

- The name of the binary
- The location of the files
- The name of the service
- The name of the config file.

WIX will take the binary and config file from the Output directory, so create it and place the files there.



```
C:\Windows\system32>cd \Users\mike\Desktop\wix
```

```
C:\Users\mike\Desktop\wix>dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 083C-9DFA
```

```
Directory of C:\Users\mike\Desktop\wix
```

```
05/28/2020  02:02 AM    <DIR>          .
05/28/2020  02:02 AM    <DIR>          ..
05/28/2020  02:02 AM                304 build_x86.bat
05/28/2020  02:02 AM                314 build.bat
05/28/2020  02:02 AM                302 build_custom.bat
05/28/2020  02:02 AM                310 build_x86_custom.bat
05/28/2020  02:02 AM            3,004 custom.xml
05/28/2020  02:02 AM            3,006 custom_x86.xml
05/28/2020  02:02 AM            2,473 README.md
05/28/2020  02:02 AM            2,766 velociraptor.xml
               8 File(s)            12,479 bytes
               2 Dir(s)  35,690,766,336 bytes free
```

```
C:\Users\mike\Desktop\wix>mkdir output
```

```
C:\Users\mike\Desktop\wix>copy ..\..\Downloads\velociraptor-v0.4.3.3-windows-amd64.exe output\velociraptor.exe
1 file(s) copied.
```

```
C:\Users\mike\Desktop\wix>copy ..\..\Downloads\client.config.yaml output\client.config.yaml
1 file(s) copied.
```



```
C:\Users\mike\Desktop\wix>build_custom.bat
```

```
C:\Users\mike\Desktop\wix>"c:\Program Files (x86)\WiX Toolset v3.11\bin\candle.exe" custom.xml -arch x64 -ext "c:\Program Files (x86)\WiX Toolset v3.11\bin\WixUtilExtension.dll"
```

```
Windows Installer XML Toolset Compiler version 3.11.2.4516
```

```
Copyright (c) .NET Foundation and contributors. All rights reserved.
```

```
custom.xml
```

```
C:\Users\mike\Desktop\wix>"c:\Program Files (x86)\WiX Toolset v3.11\bin\light.exe" custom.wixobj -ext "c:\Program Files (x86)\WiX Toolset v3.11\bin\WixUtilExtension.dll"
```

```
Windows Installer XML Toolset Linker version 3.11.2.4516
```

```
Copyright (c) .NET Foundation and contributors. All rights reserved.
```

```
C:\Users\mike\Desktop\wix>dir *.msi
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 083C-9DFA
```

```
Directory of C:\Users\mike\Desktop\wix
```

```
05/28/2020  02:06 AM          15,093,760 custom.msi
               1 File(s)          15,093,760 bytes
               0 Dir(s)  35,625,000,960 bytes free
```

```
C:\Users\mike\Desktop\wix>msiexec /i custom.msi
```

The custom msi contains the client config embedded in it.

This is the recommended way to deploy clients.



The screenshot shows a web browser window with the address bar displaying `vm1.training.velocidex.com/app.html#/search`. The application interface includes a search bar, a status indicator for 'windows-2' (connected), and a table of search results. The table has columns for Online status, ClientID, Host, OS Version, and Labels. A red box highlights the 'OS Version' column for the entry 'windows-2', which shows 'Microsoft Windows Server 2019 Datacenter10.0.17763 Build 17763'.

Online	ClientID	Host	OS Version	Labels
<input type="checkbox"/>	C.208d5bd6aaebce1b	windows-2	Microsoft Windows Server 2019 Datacenter10.0.17763 Build 17763	

After installing the MSI you should be able to see it immediately in the server's search screen.



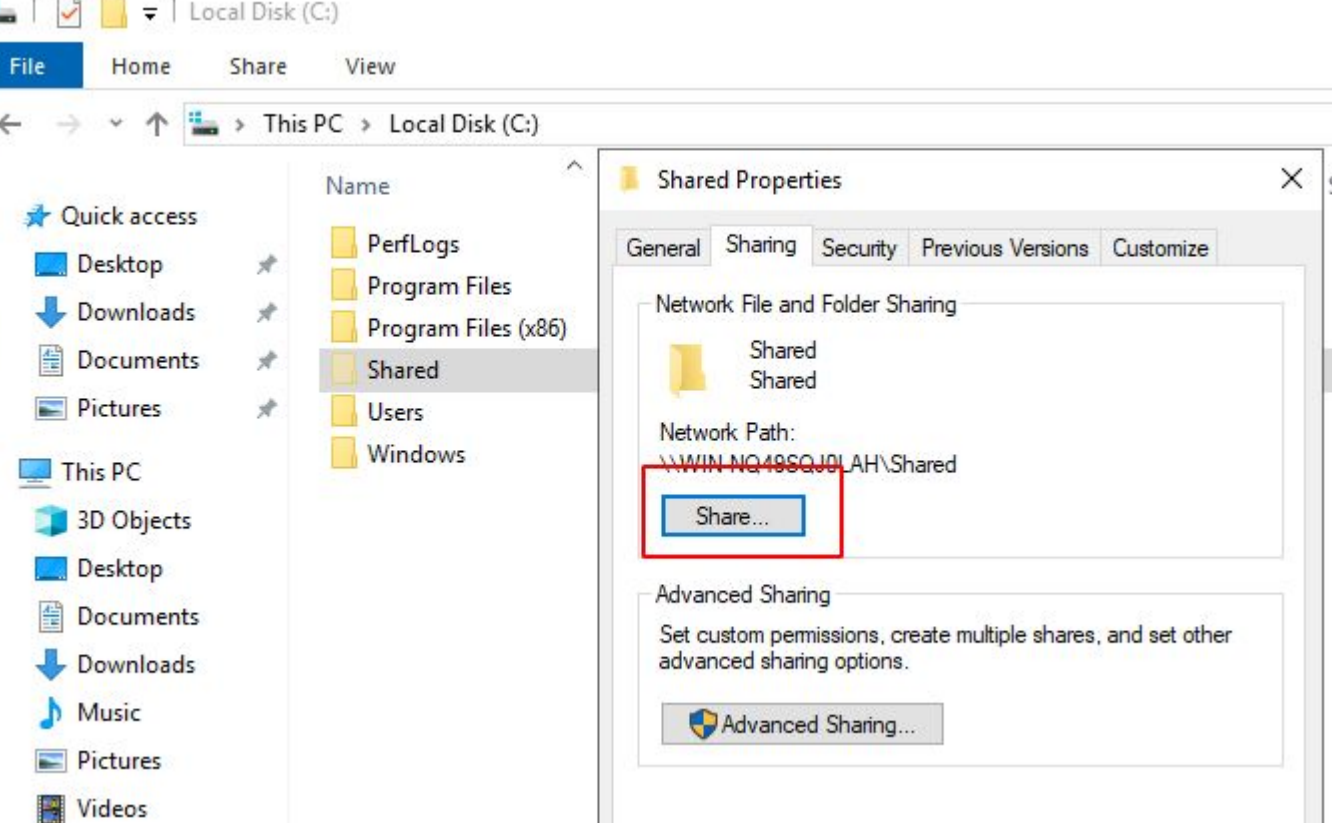
# Domain deployment

We can deploy the MSI to the entire domain using group policy.

## 2 Methods

1. Via scheduled tasks.
2. Via assigned software.





**Create a share  
to serve the  
MSI from.**

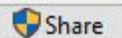


## Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write ▼
<del>Administrators</del>	<del>Owner</del>
Everyone	Read ▼

[I'm having trouble sharing](#)

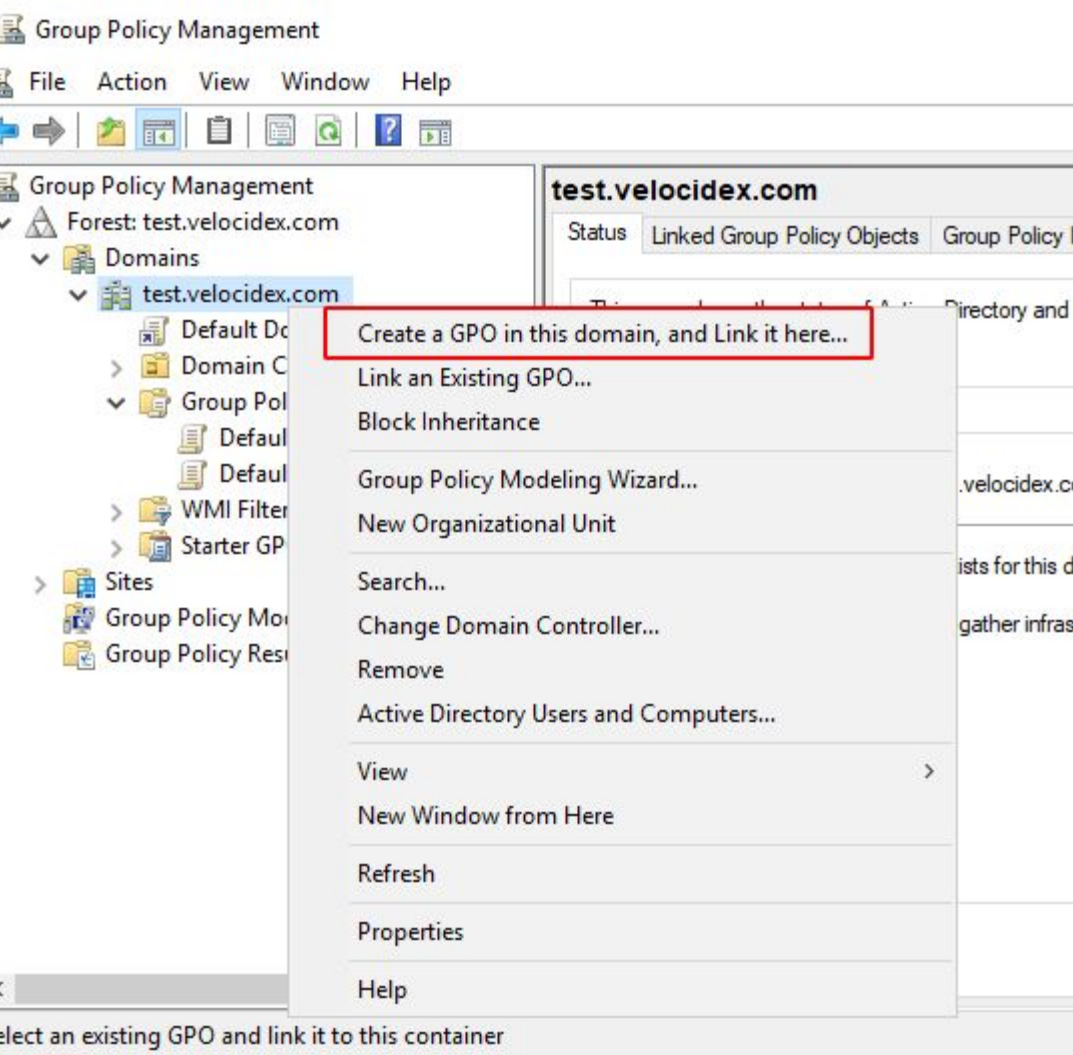


Cancel

**Ensure everyone has read access from this share - and only administrators have write access!**







**Use the group policy management tool create a new Group Policy Object in the domain (or OU)**





Group Policy Management

File Action View Window Help

Group Policy Management

- Forest: test.velocidex.com
  - Domains
    - test.velocidex.com
      - Default Domain Policy
      - Install Velociraptor
      - Domain Controllers
        - Group Policy Objects
          - Default Domain Controllers Policy
          - Default Domain Policy
          - Install Velociraptor
        - WMI Filters
        - Starter GPOs
      - Sites
      - Group Policy Modeling
      - Group Policy Results

Install Velociraptor

Scope Details Settings Delegation Status

**Links**

Display links in this location: test.velocidex.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled
test.velocidex.com	No	Yes

Edit...

GPO Status

Back Up...

Restore from Backup...

Import Settings...

Save Report...

View

New Window from Here

Copy

Delete

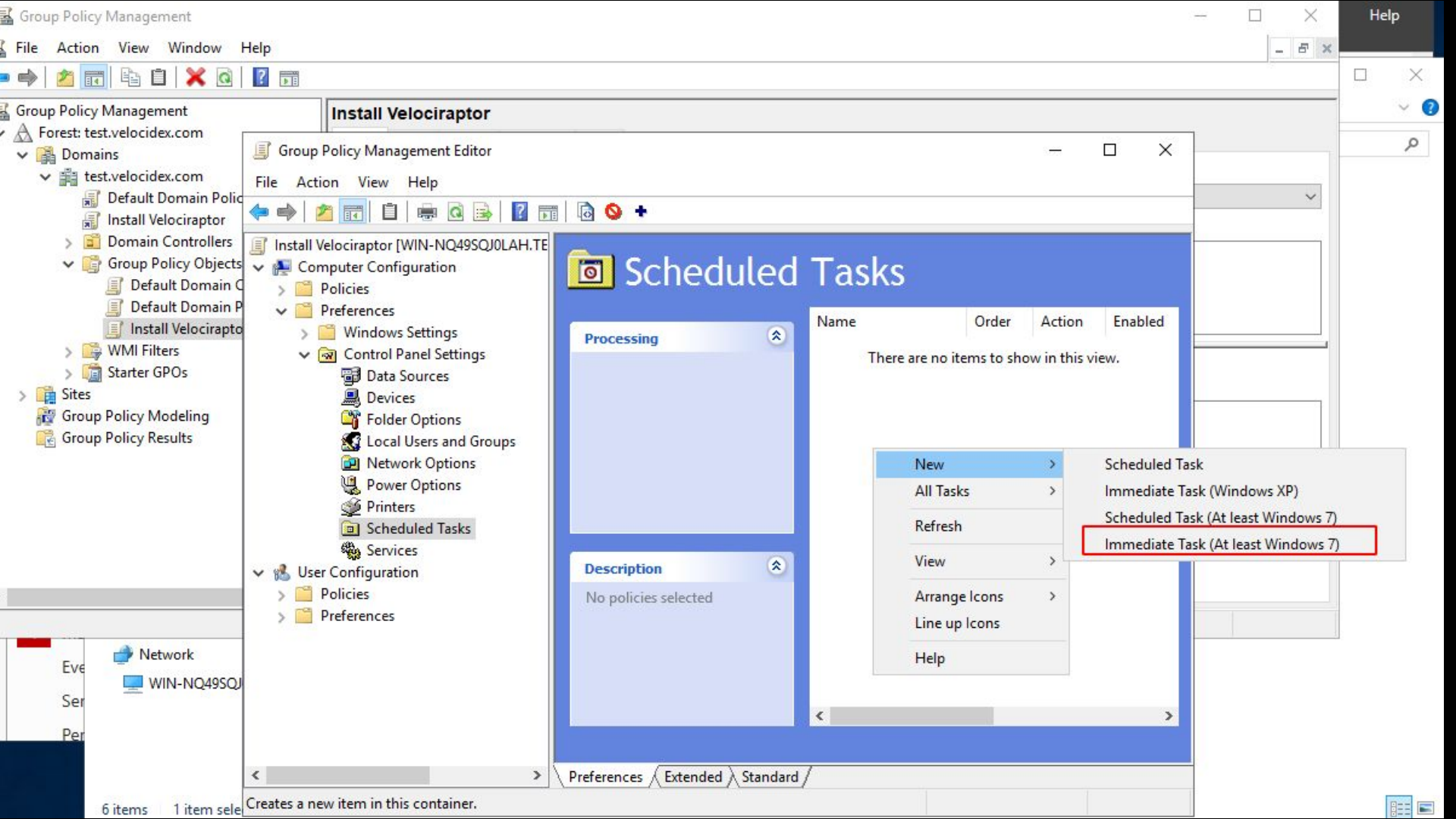
Rename

Open the GPO editor

Network

## Edit the new GPO





New Task (At least Windows 7) Properties

General Actions Conditions Settings Common

Action: Create

Name: Install Velociraptor

Author: TEST\Administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

Change User or Group...

☐ Run only when user is logged on

☒ Run whether user is logged on or not

☒ Do not store password. The task will only have access to local resources.

☒ Run with highest privileges

☐ Hidden

Configure for: Windows® 7, Windows Server™ 2008R2

OK Cancel Apply Help

Ensure the new scheduled task is run as system



When you create a task, you can specify what action this task will perform.

Action

New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script:

msiexec.exe

Browse...

Add arguments(optional):

/i \\WIN-NQ49SQJ0LAH\Shared\velociraptor.exe

Start in(optional):

New...

Edit...

OK

Cancel

Help

Using scheduled tasks you can run any binary - use this method to run interactive collection if you do not have a dedicated Velociraptor server



Options common to all items

- ☐ Stop processing items in this extension if an error occurs.
- ☐ Run in logged-on user's security context (user policy option).
- ☐ Remove this item when it is no longer applied.
- ☒ Apply once and do not reapply.
- ☐ Item-level targeting

Targeting...

Description

OK

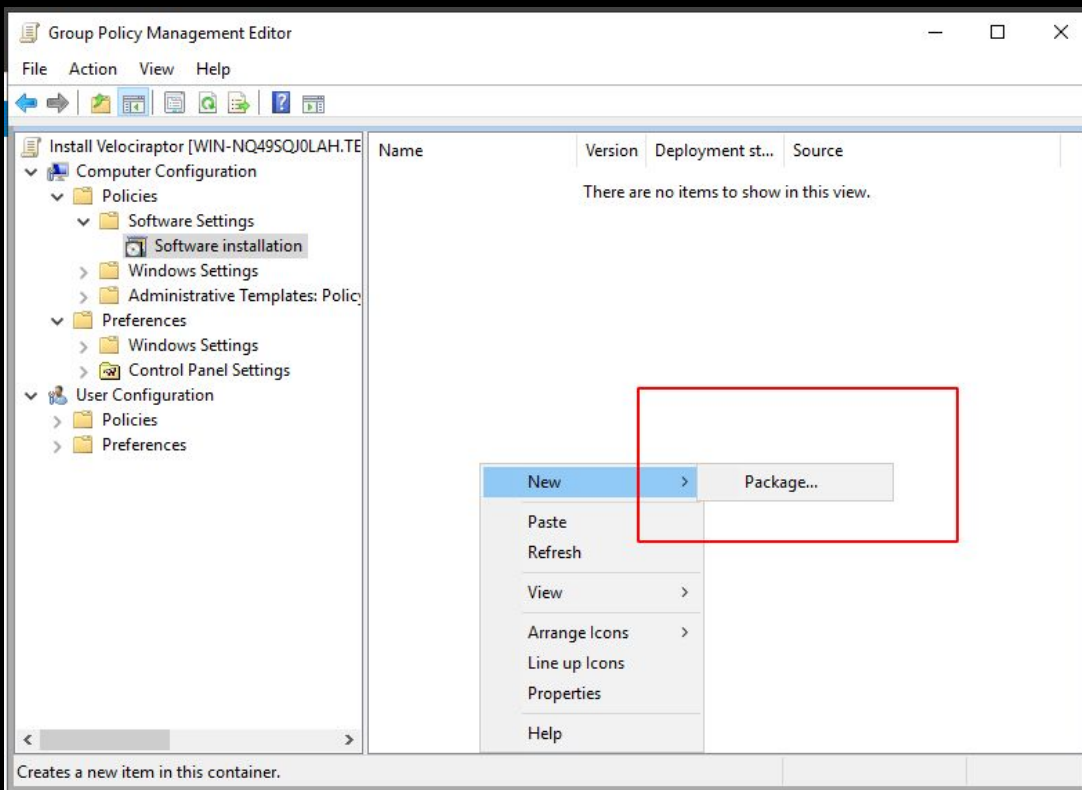
Cancel

Apply

Help

**Ensure the  
new  
scheduled  
task is run  
only once**

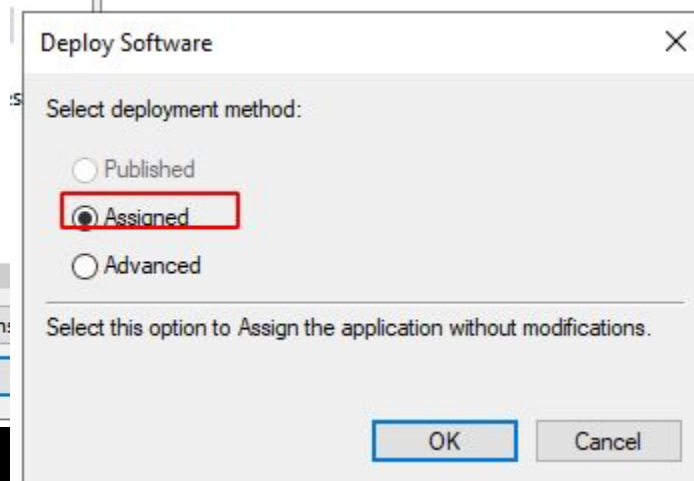
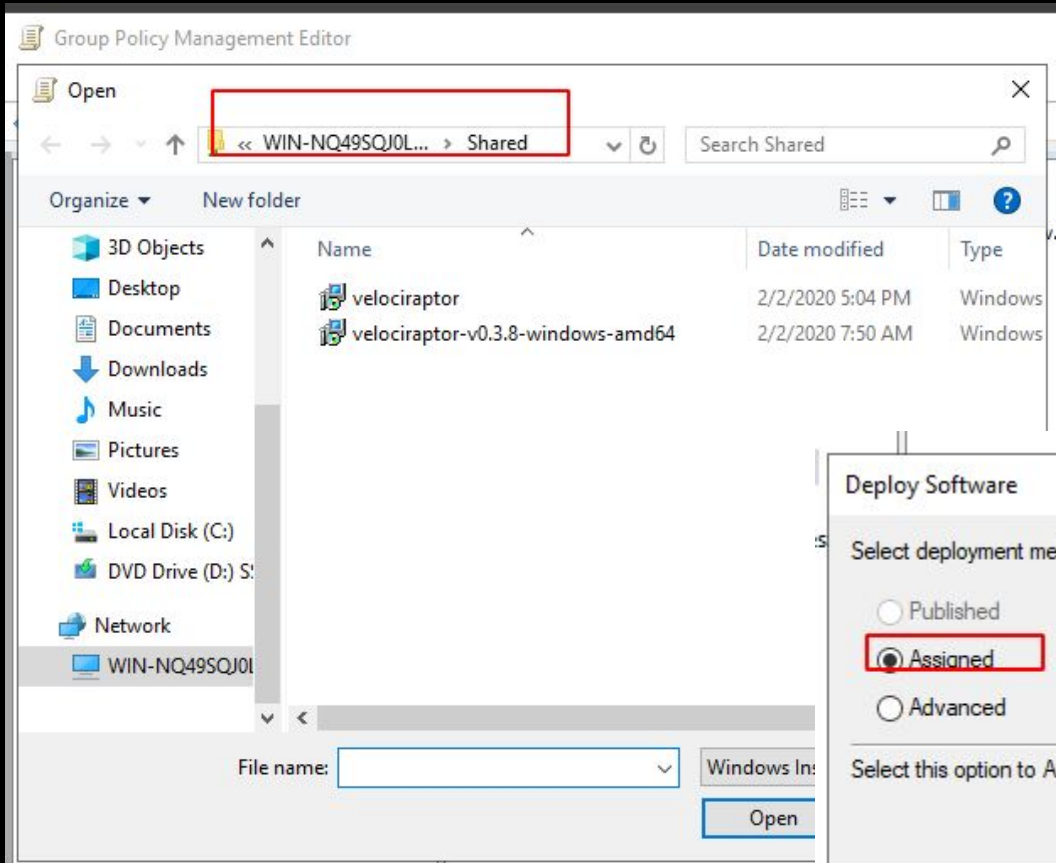




## Method 2 - install via assigned software packages in GPO

The main advantage here is that it is possible to upgrade or uninstall Velociraptor easily







Group Policy Management Editor

File Action View Help

Install Velociraptor [WIN-NQ49SQJ0LAH.TE

- Computer Configuration
  - Policies
    - Software Settings
      - Software installation
      - Windows Settings
      - Administrative Templates: Policy
    - Preferences
      - Windows Settings
      - Control Panel Settings
  - User Configuration
    - Policies
      - Software Settings
        - Software installation
        - Windows Settings
        - Administrative Templates: Policy
      - Preferences

Name	Version	Deployment st...	Source
Velociraptor	0.36	Assigned	\\WIN-NQ49SQJ0LAH\Shared\velociraptor.msi

You will need to wait until group policy is updated on the endpoint or until the next reboot. The endpoint must be on the AD LAN





# A Velociraptor GUI tour



# The Dashboard

The **Dashboard** shows the current state of the installation:

- ❑ How many clients are connected
- ❑ Current CPU load and memory footprint on the server.

When running hunts or intensive processing, memory and CPU requirements will increase but not too much.

You can customize the dashboard - it's also just an artifact.





## Welcome to Velociraptor!

### Common tasks:

- [Inspect the server's state](#)
- [Building an Offline Collector](#)
- [Write VQL notebooks](#)
- [Customize this welcome screen](#)

Or simply search for a client in the search bar above.

You can always get back to this welcome screen by clicking the little green reptile above!

### Tips

1. Press **Ctrl-/-** to view keyboard hotkeys.





Search clients



Show All



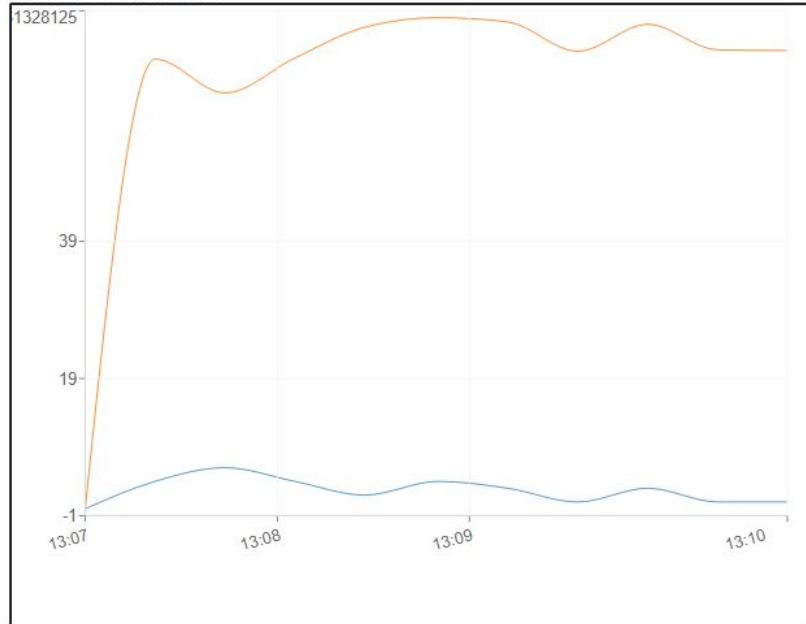
admin



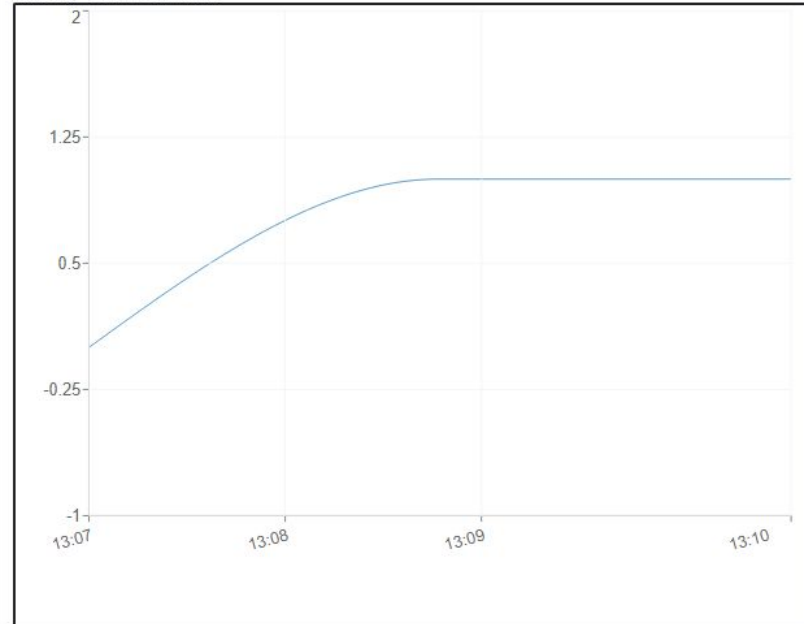
## Server status

The following are total across all frontends.

### CPU and Memory Utilization



### Currently Connected Clients



Clients have a persistent connection to the server.

They're ready to receive your commands.



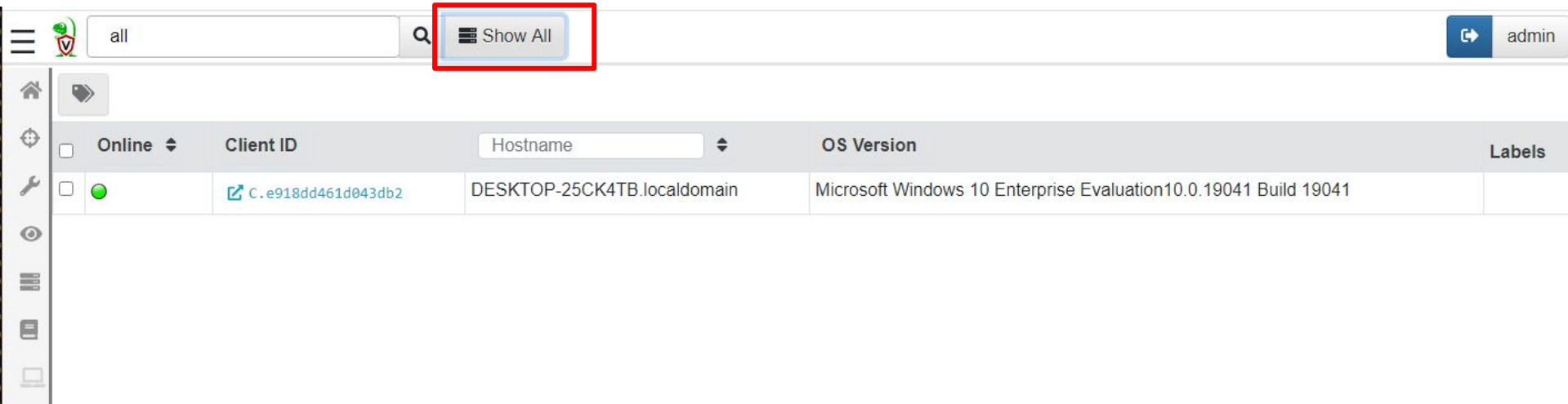
**Interactively investigate  
individual clients**



# Searching for a client

To work with a specific client we need to search for it.

Press the **Search** or **Show All** icon to see some clients



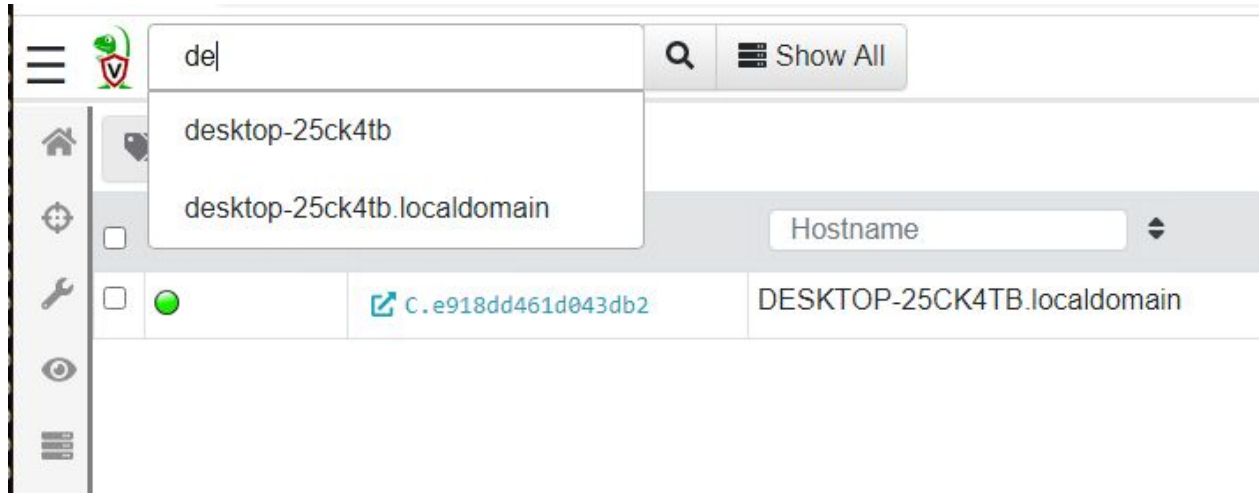
The screenshot shows the Velocidex Enterprise web interface. At the top, there is a search bar with the text "all" and a magnifying glass icon. To the right of the search bar is a button labeled "Show All" with a list icon, which is highlighted with a red rectangle. In the top right corner, there is a user profile icon and the name "admin". Below the search bar, there is a table of clients. The table has columns for "Online", "Client ID", "Hostname", "OS Version", and "Labels". The first row shows a client that is online (indicated by a green dot), with a Client ID of "C.e918dd461d043db2", a Hostname of "DESKTOP-25CK4TB.localdomain", and an OS Version of "Microsoft Windows 10 Enterprise Evaluation10.0.19041 Build 19041".

Online	Client ID	Hostname	OS Version	Labels
<input type="checkbox"/>	<a href="#">C.e918dd461d043db2</a>	DESKTOP-25CK4TB.localdomain	Microsoft Windows 10 Enterprise Evaluation10.0.19041 Build 19041	



# Search for clients hostname, label, or client ID.

You can start typing the hostname to auto-complete





# Client overview

The server collects some high level information about each endpoint.

Click **VQL Drilldown** to see more detailed information:

- ❑ Client version
- ❑ Client footprint (memory and CPU)

You can customize the information collected and shown by editing the Generic.Client.Info artifact.





de



Show All

DESKTOP-25CK4TB.localdomain

connected



admin

Interrogate

VFS

Collected

Overview

VQL Drilldown

Shell

DESKTOP-25CK4TB.localdomain

**Client ID** C.e918dd461d043db2

**Agent Version** 2020-10-22T23:03:33+10:00

**Agent Name** velociraptor

**Last Seen At** 2020-10-22 13:15:13 UTC

**Last Seen IP** 127.0.0.1:52511

**Operating System** windows

**Hostname** DESKTOP-25CK4TB.localdomain

**Release** Microsoft Windows 10 Enterprise Evaluation10.0.19041 Build 19041

**Architecture** amd64

Client Metadata

	Key	Value
+	Escalate	Bob
+	Investigator	Mike

Clients have a unique ID starting with "C.". Internally the client id is considered the most accurate source of endpoint identity

Each client has arbitrary metadata so you can integrate it easily into your procedures



DESKTOP-25CK4TB.localdomain ( C.e918dd461d043db2 ) @ 2020-10-22 06:16:14.400368928 -0700 PDT

Name	Build time	Labels	Hostname	OS	Architecture	Platform	PlatformVersion	KernelVersion	Fqdn	ADDomain
velociraptor	2020-10-22T23:03:33+10:00		DESKTOP-25CK4TB	windows	amd64	Microsoft Windows 10 Enterprise Evaluation	10.0.19041 Build 19041		DESKTOP-25CK4TB.localdomain	WORKGROUP

10 25 30 50 Showing rows 1 to 1 of 1

Memory and CPU footprint over the past 24 hours

By default, VQL Drill Down shows the recent memory and CPU load of Velociraptor on the endpoint as well as the list of users.



The GUI consists of familiar widgets: Here we can see the table widget which repeats often


This screen simply shows the report of the Generic.Client.Info artifact - you can edit the artifact to collect more/different info.












Search clients

  Show All




DESKTOP-25CK4TB.localdomain  connected

 adm

 Interrogate  VFS  Collected

 Overview  VQL Drilldown  Sheets

DESKTOP-25CK4TB.localdomain ( C.e918dd461d043db2 ) @ 2020-10-22 06:16:14.400368928 -0700 PDT

Clear All

Name

BuildTime

Labels

Hostname

OS

Architecture

Platform

PlatformVersion

KernelVersion

Fqdn

ADDomain

	Labels	Platform	PlatformVersion	KernelVersion	Fqdn	ADDomain
33+10:00		Microsoft Windows 10 Enterprise Evaluation	10.0.19041 Build 19041		DESKTOP-25CK4TB.localdomain	WORKGROUP

Showing rows 1 to 1 of 1

1

M  
OS  
U footprint over the past 24 hours

6.4

4603457-

You can show/hide columns as needed - this helps to see wider columns

## Raw Response JSON

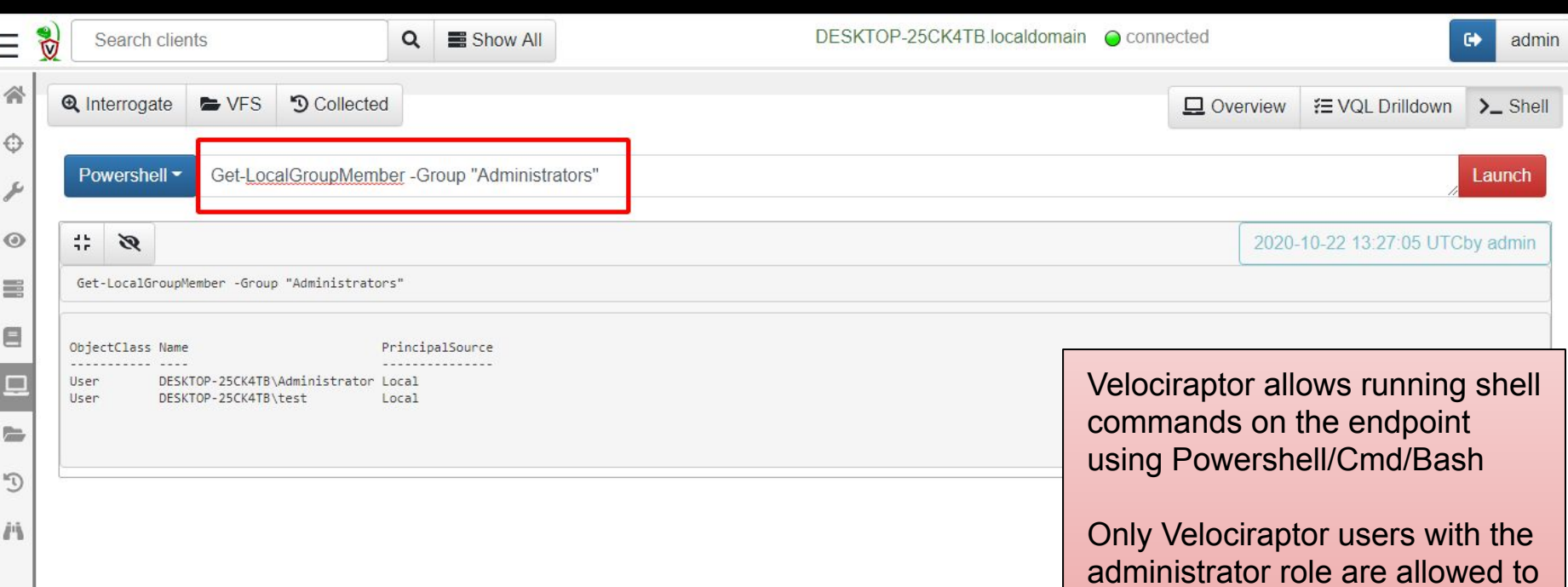
```
1 [
2   {
3     "Name": "velociraptor",
4     "BuildTime": "2020-10-22T23:03:33+10:00",
5     "Labels": null,
6     "Hostname": "DESKTOP-25CK4TB",
7     "OS": "windows",
8     "Architecture": "amd64",
9     "Platform": "Microsoft Windows 10 Enterprise Evaluation",
10    "PlatformVersion": "10.0.19041 Build 19041",
11    "KernelVersion": "",
12    "Fqdn": "DESKTOP-25CK4TB.localdomain",
13    "ADDomain": "WORKGROUP"
14  }
15 ]
```

You can see the raw data  
behind each table:

- A table is simply a list of rows
- Each row is a mapping

2020-10-22T13:24:30.11





The screenshot shows the Velociraptor web interface. At the top, there's a search bar for clients and a status bar indicating the client is connected. The main navigation bar includes tabs for Interrogate, VFS, and Collected. On the right, there are buttons for Overview, VQL Drilldown, and Shell. A red box highlights the PowerShell command input field containing `Get-LocalGroupMember -Group "Administrators"`. A Launch button is to the right of the input field. Below the input field, a timestamp shows the command was executed on 2020-10-22 at 13:27:05 UTC by admin. The output of the command is displayed in a table format.

ObjectClass	Name	PrincipalSource
User	DESKTOP-25CK4TB\Administrator	Local
User	DESKTOP-25CK4TB\test	Local

Velociraptor allows running shell commands on the endpoint using Powershell/Cmd/Bash

Only Velociraptor users with the administrator role are allowed to do this!

Actions are logged and audited

You can disable client shell ability by configuration policy - but this limits your DFIR efficacy.



**Interactively fetching  
files from the endpoint**



# The Virtual File System (VFS)

The VFS visualizes some server-side information we collect about the clients.

Top level corresponds to the type of information we collect:

- ❑ **File** - Access the file system using the filesystem API
- ❑ **NTFS** - Access the file system using raw NTFS parsing (Windows Only)
- ❑ **Registry** - Access the Windows Registry using the Registry API (Windows Only)
- ❑ **Artifacts** - A view of all artifacts collected from the client sorted by artifact type, and then times when they were collected.





# File accessor

Uses the OS APIs to access files (unless locked then it fallback to NTFS)

The screenshot displays the File Accessor application interface. The top bar shows a search field, a 'Show All' button, and the current client 'DESKTOP-25CK4TB.localdomain' with a 'connected' status. The left sidebar shows a file tree with 'Users' selected. The main area shows a table of files in the 'Users' directory. The file 'desktop.ini' is highlighted, and its details are shown in the bottom panel. The 'Download' button is highlighted in the bottom panel.

Name	Size	Mode	mtime	atime	ctime
desktop.ini	174	-rw-rw-rw-	2019-12-07T09:12:42.731564Z	2020-10-22T13:00:50.8566571Z	2019-12-07T09:14:54.4124461Z
All Users	0	Lrw-rw-rw-	2019-12-07T09:30:39.0536837Z	2019-12-07T09:30:39.0536837Z	2019-12-07T09:30:39.0536837Z

Stats Textview HexView

C:\Users\desktop.ini

Size 174

Mode -rw-rw-rw-

Mtime 2019-12-07T09:12:42.731564Z

Atime 2020-10-22T13:00:50.8566571Z

Ctime 2019-12-07T09:14:54.4124461Z

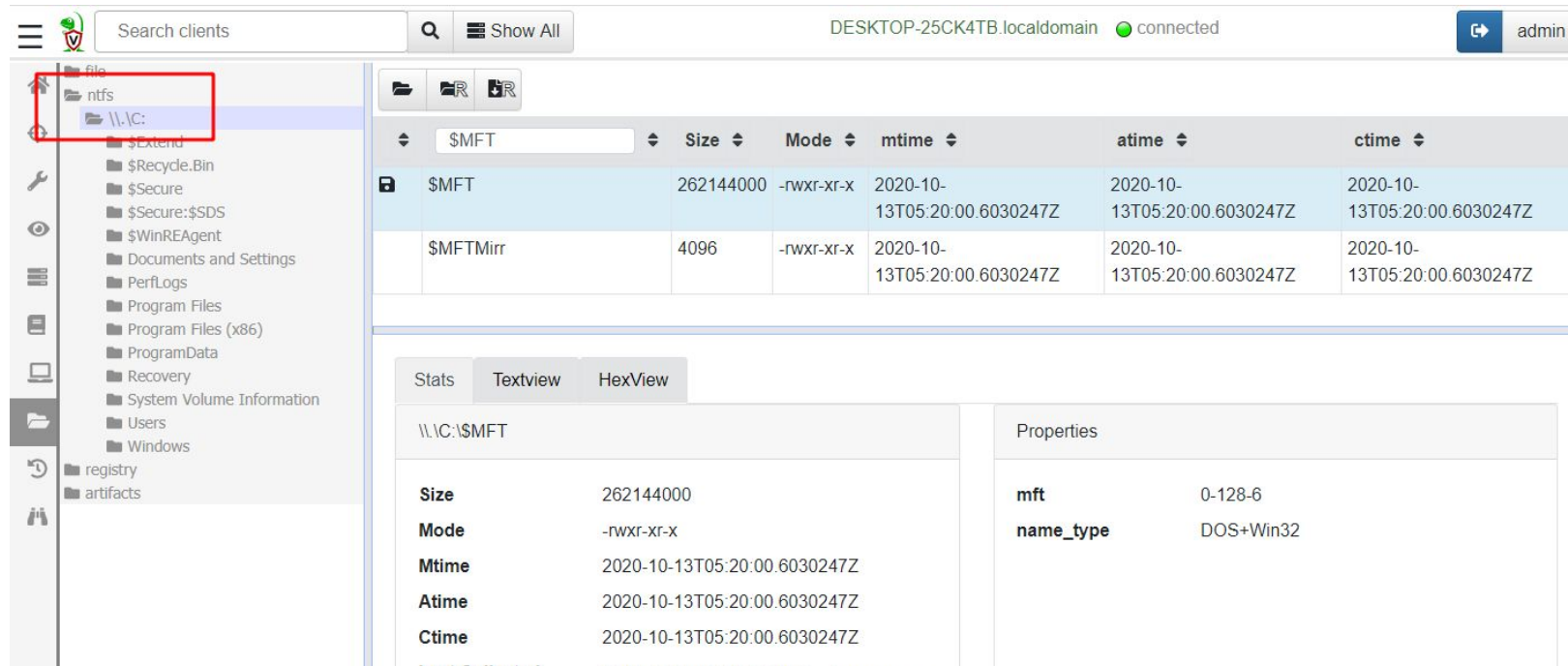
Last Collected 2020-10-22 13:28:56 UTC [Download](#)

Fetch from Client [Re-Collect from the client](#)



# NTFS Accessor

Uses raw NTFS parsing providing access to special files and ADS



Search clients    DESKTOP-25CK4TB.localdomain ● connected

File tree (left sidebar):

- file
- ntfs
- ||.C:
- \$Extend
- \$Recycle.Bin
- \$Secure
- \$Secure:\$SDS
- \$WinREAgent
- Documents and Settings
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- Recovery
- System Volume Information
- Users
- Windows
- registry
- artifacts

	Size	Mode	mtime	atime	ctime
\$MFT	262144000	-rwxr-xr-x	2020-10-13T05:20:00.6030247Z	2020-10-13T05:20:00.6030247Z	2020-10-13T05:20:00.6030247Z
\$MFTMirr	4096	-rwxr-xr-x	2020-10-13T05:20:00.6030247Z	2020-10-13T05:20:00.6030247Z	2020-10-13T05:20:00.6030247Z

Tabs: Stats | Textview | HexView

Selected item: \\.\C:\\$MFT

Properties:

- mft: 0-128-6
- name\_type: DOS+Win32

Stats details for \\.\C:\\$MFT:

- Size: 262144000
- Mode: -rwxr-xr-x
- Mtime: 2020-10-13T05:20:00.6030247Z
- Atime: 2020-10-13T05:20:00.6030247Z
- Ctime: 2020-10-13T05:20:00.6030247Z



# Registry Accessor










Provides access to registry using the Windows API.

Keys are like directories and Values are files.

Since Values are typically small, they are also retrieved as a result of a directory listing - in most cases there is no need to download content explicitly.

Note that registry mapping occurs so take care when accessing virtual keys like HKEY\_CURRENT\_USER or HKEY\_USERS





file

ntfs

\\.\C:

registry

HKEY\_CLASSES\_ROOT

HKEY\_CURRENT\_CONFIG

HKEY\_CURRENT\_USER

HKEY\_LOCAL\_MACHINE

HKEY\_PERFORMANCE\_DATA

HKEY\_USERS

.DEFAULT

S-1-5-18

Console

Control Panel

EUDC

Environment

Keyboard Layout

Printers

Software

System




S-1-5-19

S-1-5-20

S-1-5-21-1577548454-29470934

S-1-5-21-1577548454-29470934

artifacts



Name	Size	Mode	mtime	atime	ctime	btime
Path	102	-rwxr-xr-x	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z
TEMP	66	-rwxr-xr-x	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z
TMP	66	-rwxr-xr-x	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z	2019-12-07T09:15:07.4870307Z

Stats

Textview

HexView

\HKEY\_USERS\S-1-5-18\Environment\Path

Size

102

Mode

-rwxr-xr-x

Mtime

2019-12-07T09:15:07.4870307Z


Atime

2019-12-07T09:15:07.4870307Z

Ctime

2019-12-07T09:15:07.4870307Z

Fetch from Client

 Collect from the client



Properties

type



EXPAND\_SZ



value










%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;



Search clients

 Show All

DESKTOP-25CK4TB.localdomain  connected  admin



file

ntfs

registry

HKEY\_CLASSES\_ROOT

HKEY\_CURRENT\_CONFIG

HKEY\_CURRENT\_USER

HKEY\_LOCAL\_MACHINE

BCD00000000

HARDWARE

SAM

SOFTWARE

CVSM

Classes

Clients

DefaultUserEnvironment

Google

Intel

Macromedia

Microsoft

.NETFramework



ADs

ALG

AMSI

ASP.NET

AccountsControl

 Synced 246000 files 

Name	Size	Mode	mtime	atime	ctime
.NETFramework	0	drwxr-xr-x	2020-10-12T12:06:08.0719712Z	2020-10-12T12:06:08.0719712Z	2020-10-12T12:06:08.0719712Z
ADs	0	drwxr-xr-x	2019-12-07T09:15:15.2842061Z	2019-12-07T09:15:15.2842061Z	2019-12-07T09:15:15.2842061Z
ALG	0	drwxr-xr-x	2019-12-07T09:15:15.2842061Z	2019-12-07T09:15:15.2842061Z	2019-12-07T09:15:15.2842061Z
AMSI	0	drwxr-xr-x	2019-12-07T09:15:15.2842061Z	2019-12-07T09:15:15.2842061Z	2019-12-07T09:15:15.2842061Z
ASP.NET	0	drwxr-xr-x	2020-10-	2020-10-	2020-10-

Please select a file or a folder to see its details here.



# Artifacts accessor

This shows the artifacts collected from the endpoint grouped by artifact

This is useful to see the timeline of the same artifact collected at different times.



Search clients

DESKTOP-25CK4TB.localdomain connected

adm

file  
ntfs  
registry  
artifacts  
Generic.Client.Info  
F.BU8086N3BKV3S  
F.BU808DBC7M4O4  
F.BU80C7AORD792  
System.VFS.DownloadFile  
System.VFS.ListDirectory  
Windows.System.PowerShell

Name

Size

Mode

mtime

atime

ctime

BasicInformation.json

323

-r--r--r--

Users.json

1046

-r--r--r--

Stats

Textview

HexView

1

```
{ "Name": "velociraptor", "BuildTime": "2020-10-22T23:03:33+10:00",  
  "Labels": null, "Hostname": "DESKTOP-25CK4TB", "OS": "windows",  
  "Architecture": "amd64", "Platform": "Microsoft Windows 10  
Enterprise Evaluation", "PlatformVersion": "10.0.19041 Build 19041",  
  "KernelVersion": "", "Fqdn": "DESKTOP-25CK4TB.localdomain",  
  "ADDomain": "WORKGROUP" }
```

2



# Navigating the interface

Click the “Refresh this directory” will schedule a directory listing artifact and wait for the results (usually very quick if the endpoint is online).

The “Recursively refresh this directory” will schedule a recursive refresh - this may take some time! After this operation a lot of the VFS will be pre-populated already.

“Collect from client” will retrieve the file data to the server. After which, the floppy disk sign indicates that we have file data available and you can click the “Download” link to get a copy of the file.





ntu	Size	Mode	mtime	atime	ctim
NTUSER.DAT	1048576	-rw-rw-rw-	2020-10-14T08:42:07.9229959Z	2020-10-14T08:42:07.9229959Z	2020-10-14T08:42:07.9229959Z
NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}.TM.blf	65536	-rw-rw-rw-	2020-10-12T11:35:10.417672Z	2020-10-19T08:12:30.2258161Z	2020-10-12T11:35:10.417672Z
NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}.TM.blf	524288	-rw-rw-rw-	2020-10-12T11:35:10.417672Z	2020-10-19T08:12:30.2258161Z	2020-10-12T11:35:10.417672Z

## Refresh directory from endpoint (can be done recursively)

Stats    Textview    HexView

Textview

HexView

C:\Users\test\NTUSER.DAT

<b>Size</b>	1048576
<b>Mode</b>	-rw-rw-rw-
<b>Mtime</b>	2020-10-14T08:42:07.9229959Z
<b>Atime</b>	2020-10-14T08:42:07.9229959Z
<b>Ctime</b>	2020-10-12T11:34:31.5787883Z
<b>Last Collected</b>	2020-10-22 14:38:07 UTC

 Download

### Fetch from Client

 Re-Collect from the client

## Properties

Remember that the VFS view is simply a server side cache of information we know about the endpoint - it is usually out of date!

## Fetch file contents from endpoint

# Exercise: Determine user activity

**Task:** We suspect a user account had been compromised.

*Did the user download malware?*

- ❑ Freely explore the interface to answer this question
- ❑ Useful artifacts include
  - ❑ Download directory content
  - ❑ Internet browser history
  - ❑ Temporary files



desktop-ng2qvog

DESKTOP-NG2QVOG

connected

mic

Public

mike

downloads

test

%Folder%with%

3D Objects

AppData

Local

Comms

ConnectedDevice

D3DSCache

Google

Microsoft

MicrosoftEdge

OneDrive

Package Cache

Packages

PeerDistRepub

Publishers

Temp

Low

WinSAT

acl

artifact\_definitio

client\_index

clients

config

frontends

notebook\_inde:

notebooks

server\_artifacts

temp

users

VirtualStore

LocalLow

Python 3.8.1 (64-bit)\_20210119005306.log

Python 3.8.1 (64-bit)\_20210119005306\_000\_core\_AllUsers.log

Python 3.8.1 (64-bit)\_20210119005306\_001\_dev\_AllUsers.log

				23T03:06:46.1440172Z	23T03:06:46.1440172Z
Low	0	drwxrwxrwx	2021-01-01T07:58:51.891659Z	2021-01-24T13:36:22.0236895Z	
Python 3.8.1 (64-bit)_20210119005306.log	75578	-rw-rw-rw-	2021-01-19T08:54:20.2031764Z	2021-01-19T08:54:20.2031764Z	
Python 3.8.1 (64-bit)_20210119005306_000_core_AllUsers.log	87788	-rw-rw-rw-	2021-01-19T08:53:12.5169604Z	2021-01-19T08:53:12.5169604Z	
Python 3.8.1 (64-bit)_20210119005306_001_dev_AllUsers.log	341836	-rw-rw-rw-	2021-01-19T08:53:14 75140057	2021-01-19T08:53:14 75140057	

Stats

TextView

HexView

C:\Users\test\AppData\Local\Temp\Python 3.8.1 (64-bit)\_20210119005306.log

Size

75578

Mode

-rw-rw-rw-

Mtime

2021-01-19T08:54:20.2031764Z

Atime

2021-01-19T08:54:20.2031764Z

Ctime

2021-01-19T08:54:20.2031764Z

Last Collected

2021-01-24 13:40:00 UTC

Fetch from Client

Re-Collect from the client

Property

SHA256

MD5

The VFS view is similar to many other forensic packages. This makes it easier to use but it is very much less effective than writing artifacts!

95

# Velociraptor Artifacts

Fast, Efficient, Surgical



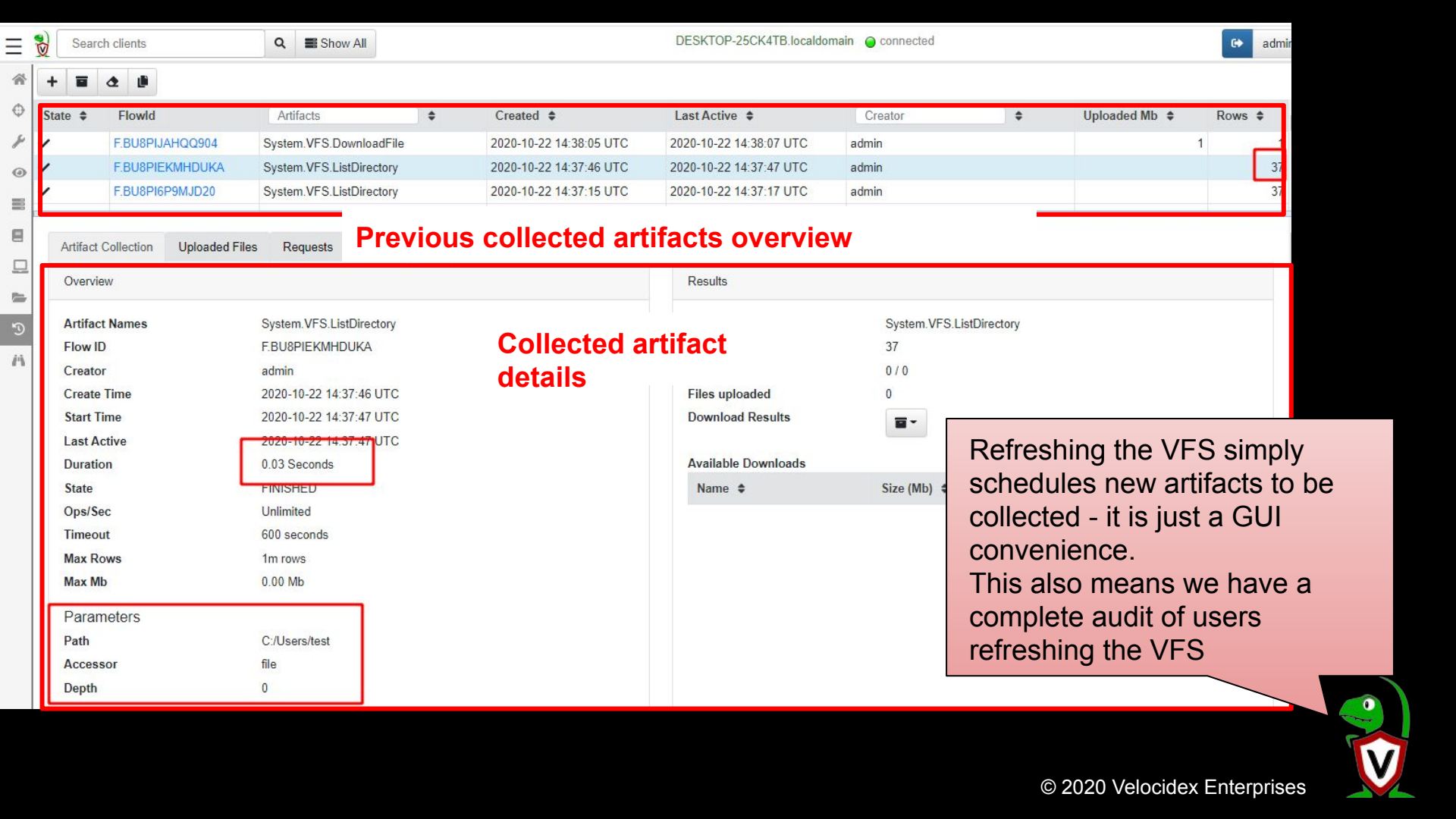
# Velociraptor artifacts

Velociraptor is just a VQL engine!

We package VQL queries in Artifacts:

- ❑ YAML files
- ❑ Include human description
- ❑ Package related VQL queries into “Sources”
- ❑ Take parameters for customization
- ❑ Can in turn be used in VQL as well...





## Previous collected artifacts overview

### Collected artifact details

Refreshing the VFS simply schedules new artifacts to be collected - it is just a GUI convenience. This also means we have a complete audit of users refreshing the VFS



# Velociraptor uses expert knowledge to find the evidence

**A key objective of Velociraptor is encapsulating DFIR knowledge into the platform, so you don't need to be a DFIR expert.**

- ❑ We have high level questions to answer
- ❑ We know where to look for evidence of user / system activities

***We build artifacts to collect and analyze the evidence in order to answer our investigative questions.***





# Velociraptor's superpower: user specified artifacts

An artifact is a YAML file ...

- ❑ (therefore user-readable, shareable and editable)
- ❑ ... that answers a question ...
- ❑ ... by collecting data from the endpoint ...
- ❑ ... and reporting on this data in a human readable way.

***Artifacts encode expert knowledge into  
human reusable components.***







## Windows.System.TaskScheduler

Type: client

The Windows task scheduler is a common mechanism that malware uses for persistence. It can be used to run arbitrary programs at a later time. Commonly malware installs a scheduled task to run itself periodically to achieve persistence.

This artifact enumerates all the task jobs (which are XML files). The artifact uploads the original XML files and then analyses them to provide an overview of the commands executed and the user under which they will be run.

### Parameters

Name	Type	Default
TasksPath		c:/Windows/System32/Tasks/**
AlsoUpload	bool	

### Source Analysis

```
1
2 LET Uploads = SELECT Name, FullPath, if(
3   condition=AlsoUpload='Y',
4   then=upload(file=FullPath)) as Upload
5 FROM glob(globs=TasksPath)
6 WHERE NOT IsDir
7
8 LET parse_task = select FullPath, parse_xml(
9   accessor='data',
10  file_name=parse/
```

## Artifact Description

## Actual VQL source

- Windows.Packs.Autoexec
- Windows.Remediation.ScheduledTasks
- Windows.System.TaskScheduler

## Artifact Search area.

Search clients | Show All | DESKTOP-25CK4TB.localdomain | connected

### New Collection: Select Artifacts to collect

task

Windows.Packs.Autoexec

Windows.Remediation.ScheduledTasks

Windows.System.TaskScheduler

#### Windows.System.TaskScheduler

Type: client

The Windows task scheduler is a common mechanism that malware uses for persistence. It can be used to run arbitrary programs at a later time. Commonly malware installs a scheduled task to run itself periodically to achieve persistence.

This artifact enumerates all the task jobs (which are XML files). The artifact uploads the original XML files and then analyses them to provide an overview of the commands executed and the user under which they will be run.

Parameters

Name	Type	Default
TasksPath		c:/Windows/System32/Tasks/**
AlsoUpload	bool	

Source Analysis

```
1
2 LET Uploads = SELECT Name, FullPath, if(
3   condition=AlsoUpload='Y',
4   then=upload(file=FullPath)) as Upload
5 FROM glob(globs=TasksPath)
```

Select Artifacts

Configure Parameters

Specify Resources

Review

Launch

To collect a new artifact, from the *Collected Artifacts* screen, click *Collect new artifact* and search for it. Select *Add* to add it to this collection. When finished simply click *Next*.





# Velociraptor Artifacts

Velociraptor comes with a large number of artifact types

1. Client Artifacts run on the endpoint
2. Client Event artifacts monitor the endpoint
3. Server Artifacts run on the server
4. Server Event artifacts monitor for events on the server.

Depending on context, the GUI artifact search screen will only show the relevant artifact types.

The **View Artifacts** page shows all types as well as details about each one.





Artifact Collection	Uploaded Files	Requests	Results	Log
---------------------	----------------	----------	---------	-----

[/clients/C.e918dd461d043db2/collections/F.BU8PNFG0HVISA/uploads/file/C:/Windows/System32/Tasks/GoogleUpdateTaskMachineCore](#)  
[/clients/C.e918dd461d043db2/collections/F.BU8PNFG0HVISA/uploads/file/C:/Windows/System32/Tasks/GoogleUpdateTaskMachineCore](#)  
[/clients/C.e918dd461d043db2/collections/F.BU8PNFG0HVISA/uploads/file/C:/Windows/System32/Tasks/OneDrive Standalone UpdateTask](#)  
[908305190-2181907579-1001](#)  
[/clients/C.e918dd461d043db2/collections/F.BU8PNFG0HVISA/uploads/file/C:/Windows/System32/Tasks/Microsoft/XblGameSaveTask](#)  
[/clients/C.e918dd461d043db2/collections/F.BU8PNFG0HVISA/uploads/file/C:/Windows/System32/Tasks/Microsoft/Windows/DUS](#)  
[/clients/C.e918dd461d043db2/collections/F.BU8PNFG0HVISA/uploads/file/C:/Windows/System32/Tasks/Microsoft/Windows/Share](#)  
[/clients/C.e918dd461d043db2/collections/F.BU8PNFG0HVISA/uploads/file/C:/Windows/System32/Tasks/Microsoft/Windows/Se](#)

You can download each one individually.

The screenshot displays the Velocidex Enterprise web interface. At the top, there is a search bar for clients and a status indicator showing 'DESKTOP-25CK4TB.localdomain' as 'connected'. Below this is a table of artifacts with columns for State, FlowId, Name, Created, Last Active, Creator, Uploaded Mb, and Rows. Two artifacts are listed: 'F.BU8PNFG0HVISA' (Windows.System.TaskScheduler) and 'F.BU8PIJAHQQ904' (System.VFS.DownloadFile). Below the artifacts table, there are tabs for 'Artifact Collection', 'Uploaded Files', 'Requests', 'Results', and 'Log'. The 'Log' tab is selected, showing a 'Client logs' section with a table of messages. The log table has columns for Timestamp, time, and message. It shows three messages related to a query execution. At the bottom of the log section, there are pagination controls showing 'Showing rows 1 to 3 of 3'.

State	FlowId	Artifacts	Created	Last Active	Creator	Uploaded Mb	Rows
✓	F.BU8PNFG0HVISA	Windows.System.TaskScheduler	2020-10-22 14:48:30 UTC	2020-10-22 14:48:39 UTC	admin	1	195
✓	F.BU8PIJAHQQ904	System.VFS.DownloadFile	2020-10-22 14:38:05 UTC	2020-10-22 14:38:07 UTC	admin	1	1

Timestamp	time	message
2020-10-22 14:48:30 UTC	2020-10-22 07:48:30 -0700 PDT	vql: Starting query execution.
2020-10-22 14:48:39 UTC	2020-10-22 07:48:39 -0700 PDT	Time 1: Windows.System.TaskScheduler/Analysis: Sending response part 0 238 kB (195 rows).
2020-10-22 14:48:39 UTC	2020-10-22 07:48:39 -0700 PDT	Uploaded 195 files.

As the query is running on the endpoint any log messages are sent to the server. Click the log tab to see if there were any errors and how many rows are expected.





desktop-ng2qvog

DESKTOP-NG2QVOG connected

mic

State FlowId Artifacts Created Last Active Creator Mb Rows

✓	F.C0555QFN5V9RM	Windows.Forensics.Prefetch Windows.Sys.Users	2021-01-22 04:22:01 UTC	2021-01-22 04:22:05 UTC	mic		237
✓	F.C0555953O9KM6	Windows.System.TaskScheduler	2021-01-22 04:20:52	2021-01-22 04:20:55	mic	1	195

Artifact Collection Uploaded Files Requests Results Log Notebook

Windows.Sys.Users  
Windows.Sys.Users  
Windows.Forensics.Prefetch

**Source Selector**

Uid	Gid	Name	Description	Directory	UUID
500	513	Administrator	Built-in account for administering the computer/domain	[ ]	S-1-5-21-1577548454-2947093465-2871365475-500
503	513	DefaultAccount	A user account managed by the system.	[ ]	S-1-5-21-1577548454-2947093465-2871365475-

Viewing the result tab shows the **rows sent** from every artifact and source.





desktop-ng2qvog

DESKTOP-NG2QVOG

connected

+

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.C0555QFN5V9RM	Windows.Forensics.Prefetch Windows.Sys.Users	2021-01-22 04:22:01 UTC	2021-01-22 04:22:05 UTC	mic		237
✓	F.C0555953O9KM6	Windows.System.TaskScheduler	2021-01-22 04:20:52	2021-01-22 04:20:55	mic	1	195

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

Overview

Extract

+

DESKTOP-NG2QVOG-C.56505d2ba2d63ace-F.C0555QFN5V9RM.zip

Q

-

x

<

>

🏠

Location: /clients/DESKTOP-NG2QVOG/artifacts/Windows.Forensics.Prefetch/

DESKTOP-NG2QVOG-C.56505d2ba...

clients

DESKTOP-NG2QVOG

artifacts

Windows.Forensics.Prefetch

Windows.Sys.Users

collections

F.C0555QFN5V9RM

Name	Size	Type	Mb
F.C0555QFN5V9RM.csv	58.5 kB	CSV document	01
F.C0555QFN5V9RM.json	88.9 kB	JSON document	01

Ops/Sec

Unlimited

Timeout

600 seconds

Max Rows

1m rows

Max Mb

1000.00 Mb

Parameters

Results

Artifacts with Results

Windows.Sys.UsersWindows.Forensics.Prefetch

Total Rows

237

Uploaded Bytes

0 / 0

Files uploaded

0

Download Results

Available Downloads

Prepare Download

Prepare Collection Report

Name	(Mb)	Date
DESKTOP-NG2QVOG-C.56505d2ba2d63ace-F.C0555QFN5V9RM.zip	0	2021-01-22T04:26:11Z



State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.C05595IEKLBNM	Windows.KapeFiles.Targets	2021-01-22 04:29:10 UTC	2021-01-22 04:29:15 UTC	mic	67	296
✓	F.C0555QFN5V9RM	Windows.Forensics.Prefetch Windows.Sys.Users	2021-01-22 04:22:01 UTC	2021-01-22 04:22:05 UTC	mic		237

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

Uploaded Files



Timestamp	started	vfs_path	file_size	uploaded_size
1611289753	2021-01-22 04:29:13.876873785 +0000 UTC	/clients/C.56505d2ba2d63ace/collections/F.C05595IEKLBNM/uploads/auto/C:/Windows/System32/winevt/Logs/HardwareEvents.evtx	69632	69632
1611289753	2021-01-22 04:29:13.876889892 +0000 UTC	/clients/C.56505d2ba2d63ace/collections/F.C05595IEKLBNM/uploads/auto/C:/Windows/System32/winevt/Logs/Internet Explorer.evtx	69632	69632
1611289753	2021-01-22 04:29:13.876896039 +0000 UTC	/clients/C.56505d2ba2d63ace/collections/F.C05595IEKLBNM/uploads/auto/C:/Windows/System32/winevt/Logs/Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx	69632	69632
1611289753	2021-01-22	/clients/C.56505d2ba2d63ace/collections/F.C05595IEKLBNM/uploads/auto/C:/Windows/System32/winevt/Logs/Key Management	69632	69632



# Searching, Viewing and Modifying artifacts







# View artifacts

Artifacts are just YAML files

The “View Artifacts” screen allows users to explore the different available artifacts.

While most users will just collect existing ones, we expect power users to customize and write their own artifacts from scratch.





Windows.System.TaskScheduler

Type: client

The Windows task scheduler is a common mechanism that malware uses for persistence. It can be used to run arbitrary programs at a later time. Commonly malware uses the task scheduler to achieve persistence.


This artifact enumerates all the task jobs (which are XML files). The artifact uploads the original XML files and then analyses them to provide an overview of the commands executed and the user under which they will be run.

Parameters

Name	Type	Default
TasksPath		c:/Windows/System32/Tasks/**
AlsoUpload		

Source Analysis

```
1
2 LET Uploads = SELECT Name, FullPath, if(
3   condition=AlsoUpload='Y',
4   then=upload(file=FullPath)) as Upload
5 FROM glob(globs=TasksPath)
6 WHERE NOT IsDir
7
8 LET parse_task = select FullPath, parse_xml(
9   accessor='data',
10  file=regex_replace(
11    source=utf16(string=Data),
```

 task

Windows.Packs.Autoexec

Windows.Remediation.ScheduledTasks

Windows.System.TaskScheduler

Search box

## Edit Windows.System.TaskScheduler

```
1 name: Custom.Windows.System.TaskScheduler
2 description: |
3   The Windows task scheduler is a common mechanism that malware uses
4   for persistence. It can be used to run arbitrary programs at a later
5   time. Commonly malware installs a scheduled task to run itself
6   periodically to achieve persistence.
7
8   This artifact enumerates all the task jobs (which are XML
9   files). The artifact uploads the original XML files and then
10  analyses them to provide an overview of the commands executed and
11  the user under which they will be run.
12
13 parameters:
14   - name: TasksPath
15     default: c:/Windows/System32/Tasks/**
16   - name: AlsoUpload
17     type: bool
18
19 sources:
20   - name: Analysis
```

User artifacts must have the prefix "Custom.". You can collect the original or the customized version as you please.

Close Save

2020-10-22T15:02:29.61



# Customizing the dashboard

The main server dashboard is just an artifact called **Server.Monitor.Health !**

You can therefore modify it.

I usually put the name of the deployment prominently and/or links to MSI or client config files - we have so many different deployments it is hard to keep track!





Search clients Q Show All DESKTOP-25CK4TB.localdomain connected

### Edit Server.Monitor.Health

```
33 {{ define "CurrentConnections" }}
34     SELECT * FROM sample(
35         n=atoi(string=Sample),
36         query={
37             SELECT _ts as Timestamp,
38                 client_comms_current_connections
39             FROM source(source="Prometheus",
40                 artifact="Server.Monitor.Health")
41         })
42     {{ end }}
43
44 ## Server status (My Special Server)
45
46 <p>The following are total across all frontends.</p>
47 <span class="container">
48     <span class="row">
49         <span class="col-sm panel">
50             CPU and Memory Utilization
51             {{ Query "CPU" | LineChart "xaxis_mode" "time" "RSS.yaxis" 2 }}
52         </span>
```

Close Save

2020-10-22T15:04:00.60







The template contains markdown composed from Golang Template Language. You can also run VQL in dashboards!



Hunting everywhere



# Hunting

Collecting the same artifact from many endpoints is called “hunting”.

A hunt is just a logical container for many individual collections

- ❑ You can download all collections at the same time
- ❑ You can see how many endpoints participated
- ❑ You can select which machines will participate based on labels, OS or other conditions.



# Hunting

Velociraptor hunts are always active until they expire  
Endpoints not currently online will receive the hunt when they check in next.

Therefore the result set is always changing - you can prepare a new download to obtain the latest version of the hunt results.

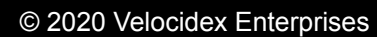


## Exercise - collect tasks everywhere

Repeat the previous artifact collection as a hunt.

This captures the state of the deployment at a point in time when the hunt was collected.



2020-10-22T14:55:48.61

desktop-no2qvoa    Show All    DESKTOP-NG2QVOG    connected

## New Hunt - Configure Hunt

Description: Hunt For all Scheduled tasks

Expiry: 1/29/2021 2:31 PM

Include Condition: Match by label

Include Labels: Select some items...

Exclude Condition:

- ☒ first
- ☐ Select All
- ☐ firstlabel

23

Configure Hunt   Select Artifacts   Configure Parameters   Specify Resources   Review   Launch

Velociraptor just collects artifacts - the artifact selection GUI is a repeating theme that works the same way in different contexts!

You can target hunts at specific label groups or OS.



## Create Hunt: Select artifacts to collect

[Windows.Packs.Autoexec](#)[Windows.Remediation.ScheduledTasks](#)[Windows.System.TaskScheduler](#)

### Windows.System.TaskScheduler

Type: client

The Windows task scheduler is a common mechanism that malware uses for persistence. It can be used to run arbitrary programs at a later time. Commonly malware installs a scheduled task to run itself periodically to achieve persistence.

This artifact enumerates all the task jobs (which are XML files). The artifact uploads the original XML files and then analyses them to provide an overview of the commands executed and the user under which they will be run.

#### Parameters

Name	Type	Default
TasksPath		c:/Windows/System32/Tasks/**

AlsoUpload bool

#### Source Analysis

```
1
2 LET Uploads = SELECT Name, FullPath, if(
3   condition=AlsoUpload='Y',
4   then=upload(file=FullPath)) as Upload
5 FROM glob(globs=TasksPath)
```

[Configure Hunt](#)[Select Artifacts](#)[Configure Parameters](#)[Specify Resources](#)[Review](#)[Launch](#)

2020-10-22T14:56:24.61





Search clients

DESKTOP-25CK4TB.localdomain connected

admin

Run this hunt?

Are you sure you want to run this hunt?

Close Run it!

State	Hunt ID	Description	Limit	Scheduled	Creator
PAUSED	H.5bed8104	Task schedule hunt		2020-10-17 17:10:24 UTC	admin

Overview Requests Results Clients Status

Overview

**Artifact Names** Windows.System.TaskScheduler

**Hunt ID** H.5bed8104

**Creator** admin

**Creation Time** 2020-10-22 14:56:57 UTC

**Expiry Time** 52798-03-17 17:10:24 UTC

**State** PAUSED

**Ops/Sec** Unlimited

Parameters

**Results**

**Total scheduled**

**Finished clients** 0

**Download Results**

**Available Downloads**

name	size	date
------	------	------



desktop-ng2qvog

DESKTOP-NG2QVOG connected

mic

State	Hunt ID	Description	Created	Started	Expires	Limit	Scheduled	Creator
	H.d12438e6	Hunt For all Scheduled tasks	2021-01-22 04:46:04 UTC	2021-01-22 04:46:20 UTC	2021-01-29 04:46:00 UTC		2001	mic
	H.a8fb5253	a8fb	2021-01-19 04:20:29 UTC	2021-01-19 07:08:54 UTC	2021-01-26 04:19:54 UTC		4002	mic
	H.84858371	848	2021-01-19 03:30:53 UTC	2021-01-19 03:30:53 UTC	2021-01-26 03:30:53 UTC		2000	mic
	H.4c1cee7b	System.VFS.ListDirectory	2021-01-19 01:48:59 UTC	2021-01-19 01:49:03 UTC	2021-01-26 01:48:46 UTC		4002	mic

Overview

Requests

Clients

Notebook

Overview

Results

Artifact Names

Hunt ID

Creator

Creation Time

Expiry Time

State

Ops/Sec

Windows.System.TaskScheduler

H.d12438e6

mic

2021-01-22 04:46:04 UTC

2021-01-29 04:46:00 UTC

RUNNING

Unlimited

Parameters

Windows.System.TaskScheduler

Total scheduled

Finished clients

Download Results

2001

402

Available Downloads

name

size

date

© 2020 Velocidex Enterprises

Extract

+

H.d12438e6.zip

mic

< > Home

Location: /All Windows.System.TaskScheduler/

H.d12438e6.zip

All Windows.System.TaskScheduler

clients

DESKTOP-NG2QVOG

artifacts

Windows.System.TaskSchedu...

F.C055HA605LDR0

collections

F.C055HA605LDR0

DESKTOP-NG2QVOG-1

artifacts

Windows.System.TaskSchedu...

F.C055H920R7C46

collections

Name	Size	Type	Modified
Analysis.json	511.0 MB	JSON doc...	01 January 1970, 10:00

Artifact Names

Windows.System.TaskScheduler

Hunt ID

H.d12438e6

Creator

mic

Creation Time

2021-01-22 04:46:04 UTC

Expiry Time

2021-01-29 04:46:00 UTC

State

RUNNING

Ops/Sec

Unlimited

Parameters

Windows.System.TaskScheduler

Total scheduled

2001

Finished clients

2001

Download Results

Available Downloads

name	size
H.d12438e6.zip	161061384

When hunting large numbers of endpoints data grows quickly!



+

▶

■

📄

📁

📤

🗑️

📄

📤

Overview

Requests

Clients

Notebook

🗑️

🔧

📄

📤

VQL

```
5 SELECT * , count() AS Count
4 FROM hunt_results(
3     artifact='Windows.System.TaskScheduler/Analysis',
2     hunt_id='H.C26MFTPBV2M9I')
1 WHERE Command =~ "cmd.exe"
6 GROUP BY Command, Arguments
```

📄

🔧

📄

📤

FullPath	Command	Arguments	ComHandler	Userld	Flowld	Clientld	Fqdn	Count
C:\Windows\System32\Tasks\Microsoft\Windows\Workplace Join\Automatic-Device-Join	%SystemRoot%\System32\dsregcmd.exe	\$(Arg0) \$(Arg1) \$(Arg2)		S-1-5-18	F.C26MG0INHRR9C	C.b5e149830d130b13	DESKTOP-VBCQLNM-381	1000
C:\Windows\System32\Tasks\Microsoft\Windows\Workplace Join\Recovery-Check	%SystemRoot%\System32\dsregcmd.exe	/checkrecovery			F.C26MG0INHRR9C	C.b5e149830d130b13	DESKTOP-VBCQLNM-381	1000
C:\Windows\System32\Tasks\T1053_005_OnLogon	cmd.exe	/c calc.exe		DESKTOP-VBCQLNM\test	F.C26M			

10

25

30

50

Showing rows 1 to 3 of 3

« 0 »

Goto Page

You can post process the hunt results directly in the hunt notebook

Query Stats: {"RowsScanned":196000,"PluginsCalled":1,"FunctionsCalled":3000,"ProtocolSearch":0,"ScopeCopy":395001}



# The Velociraptor Reverse Proxy

Velociraptor has a built in reverse proxy

- ❑ This allows us to serve other web applications through the Velociraptor server. Velociraptor will take care of authentication and SSL for free.
- ❑ It is useful to export the filestore so users can just download the files they want.



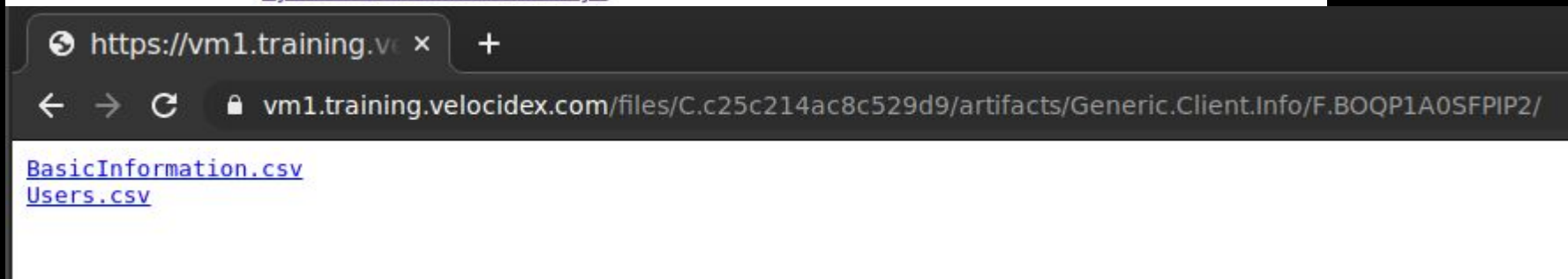
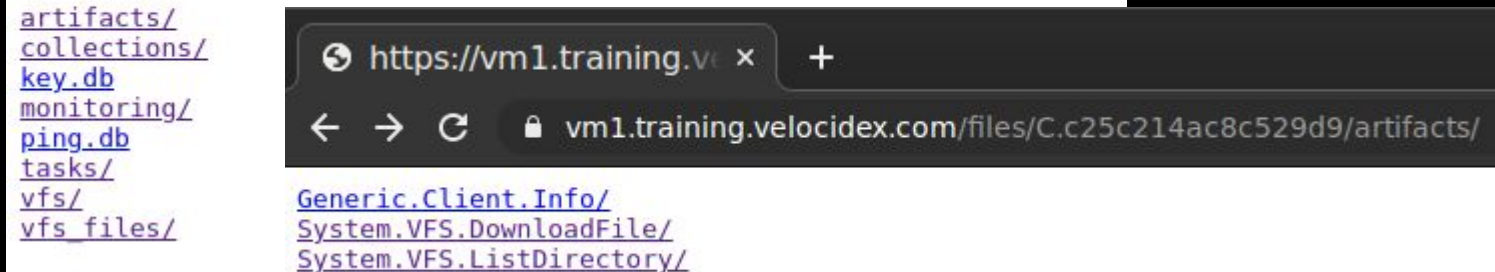
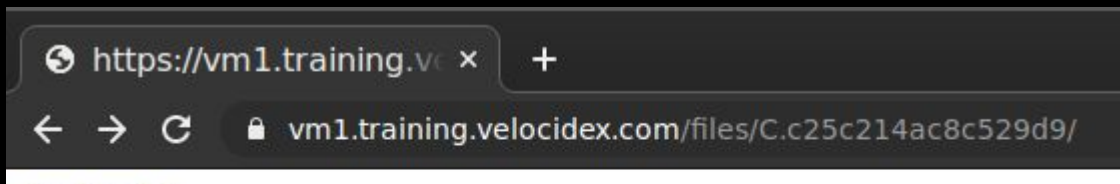
# Export the file store over HTTPS

GUI:

```
reverse_proxy:  
- route: /files/  
  url: file:///var/tmp/velociraptor/clients/  
  require_auth: true
```

```
root@server-1:/home/mike# vi /etc/velociraptor/server.config.yaml  
root@server-1:/home/mike# service velociraptor_server restart  
root@server-1:/home/mike# service velociraptor_server status  
● velociraptor_server.service - Velociraptor linux amd64  
   Loaded: loaded (/etc/systemd/system/velociraptor_server.service; enabled; vendor preset: enabled)  
   Active: active (running) since Mon 2020-02-03 02:05:56 UTC; 938ms ago  
 Main PID: 24029 (velociraptor)  
    Tasks: 7 (limit: 4915)  
   CGroup: /system.slice/velociraptor_server.service  
           └─24029 /usr/local/bin/velociraptor --config /etc/velociraptor/server.config.yaml frontend  
  
Feb 03 02:05:56 server-1 systemd[1]: Started Velociraptor linux amd64.
```

Browse the internal file store and note the location of different files.





# Double check your security

It is **really** important that auth is required!

Test this twice!

Try to get one of the URLs with no authentication using curl - it should redirect to the auth screen.

```
root@server-1:/home/mike# curl https://vm1.training.velocidex.com/files/C.81bf6660b9db0193/artifacts/  
<a href="/auth/google/login">Temporary Redirect</a>.
```

```
root@server-1:/home/mike# curl https://vm1.training.vel  
<a href="/auth/google/login">Temporary Redirect</a>.
```





# Conclusions

In this module we introduced Velociraptor - a powerful endpoint visibility solution

We mentioned that Velociraptor is based on VQL - a flexible query language

We installed Velociraptor in a cloud deployment, prepared custom MSI packages and distributed them using group policy to our endpoints.



# Conclusions

We introduced the Velociraptor GUI

- ❑ The Virtual Filesystem abstraction (VFS) provides server side caching of the client's filesystem
  - ❑ We can navigate and refresh our view of the client's filesystem in a familiar way.
- ❑ We learned about artifacts as a way of encapsulating VQL queries in a human readable, functionally focused YAML file.



# Conclusions

- ❑ We learned how artifacts can be collected from one end point
  - ❑ Exporting the collection into a zip file can archive the files collected and query results as CSV files.
- ❑ Leveling up, we can collect the same artifact from many systems. This is called a hunt.
  - ❑ Exporting the hunt as a Zip file allows large collections to be archived as a snapshot from the entire deployment.

